REQUEST FOR PROPOSAL
FOR
SELECTION OF SYSTEM INTEGRATOR (SI)
FOR DESIGN, DEVELOPMENT, IMPLEMENTATION AND MAINTENANCE OF
PFRDA-TRACE
(Tracking Reporting Analytics & Compliance e-Platform)

RFP Reference No: PFRDA/2024/TARCH/PFRDA-TRACE/01

Dated: 31st January 2024

Tender Issuing Authority

PENSION FUND REGULATORY AND DEVELOPMENT AUTHORITY(PFRDA)
B-14/A, Qutab Institutional Area, Chhatrapati Shivaji Bhavan, Katwaria Sarai, New Delhi-110016

Table of Contents

1. Disclaimer

1. The information contained in this RFP is selective and is subject to updating, expansion, revision and amendment at the sole discretion of PFRDA. The information contained in this RFP or provided subsequently to Bidder(s) in documentary form/email by or on behalf of PFRDA, shall be deemed to be part of this RFP.
2. The purpose of this RFP is to provide the interested Bidder(s) with information to assist them in preparation of their Bid proposals. This RFP does not claim to contain all the information each Bidder may require. Each Bidder should conduct its own investigations and analysis and should check the accuracy, reliability and completeness of the information contained in this RFP and where necessary obtain independent advice/clarifications, at their own cost. PFRDA may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFP to get the best proposal.
3. PFRDA, or any of its officers or employees, or any of their advisers/consultants makes no representation or warranty and shall have no liability to any person, including any Bidder under any law, statute, rules or regulations or tort, principles of restitution or unjust enrichment or otherwise for any loss, damages, cost or expense which may arise from or be incurred or suffered on account of anything contained in this RFP or otherwise, including the accuracy, adequacy, correctness, completeness or reliability of the RFP and any assessment, assumption, statement or information contained therein or deemed to form or arising in any way for participation in this bidding process by bidders.
4. PFRDA also accepts no liability of any nature whether resulting from negligence or otherwise, howsoever caused from reliance of any Bidder upon the statements contained in this RFP.
5. Bidders are presumed to have examined all instructions, forms, terms, and specifications in this RFP along with the eligibility conditions as on the date of submission of its bid. Failure to furnish all information required under this RFP or to submit a Bid not substantially responsive to this RFP in all respect will be at bidder's risk and may result in rejection of the Bid.
6. This RFP is not an offer by PFRDA but an invitation to receive proposals/bids from interested and eligible bidders for selection of System Integrator for the design, development, and maintenance of the project for PFRDA.
7. No contractual obligation whatsoever shall arise from the RFP process unless and until a formal contract is executed between PFRDA and the successful bidder. PFRDA reserves the right to cancel the selection process at any stage, prior to the appointment of System Integrator and signing the contract, without any liability owed to any party.
8. This RFP is being issued with no financial commitment and PFRDA reserves the right to withdraw the RFP and change or vary any part thereof or foreclose the same at any stage.

9. This RFP document shall not be transferred, reproduced, or otherwise used for purpose other than for which it is specifically issued.

2. Abbreviations

#	Abbreviation	Explanation
1	AMC	Annual Maintenance Contract
2	API	Application Programming Interface
3	BOM	Bill of Material
4	BPR	Business Process Re-engineering
5	CERT-In	Indian Computer Emergency Response Team
6	CI CD	Continuous integration and continuous delivery/Continuous deployment
7	Cloud DC-DR	Cloud Data Centre- Disaster Recovery
8	CMMI	Capability Maturity Model Integration
9	CRAs	Central Record Keeping Agencies
10	CRM	Customer Relationship Management
11	DB	Database
12	DXP	Digital Experience Platform
13	EMD	Earnest Money Deposit
14	ERP	Enterprise Resource Planning
15	FRS	Functional Requirement Specification
16	FSDC	Financial Stability and Development Council
17	FSLRC	Financial Sector Legislative Reforms Commission
18	GB	Giga Byte
19	GCC	Government Community Cloud
20	GIGW	Government of India guidelines for websites
21	GIS	Geographic Information System
22	HBIDS	Host Based Intrusion Detection System
23	IOPS	Input/ Output Operations Per Second
24	IRDAI	Insurance Regulatory and Development Authority of India
25	ISO	International Organization for Standardization
26	LMS	Learning Management System
27	MFA	Multi Factor Authentication
28	NBIDS	Network Based Intrusion Detection System
29	NCFE	National Centre for Financial Education

#	Abbreviation	Explanation
30	NIC	National Informatics Centre
31	NO SQL	Not Only SQL
32	NOC	Network Operations Centre
33	OWASP	Open Worldwide Application Security Project
34	OWASP Top 20	Top 20 OWASP Vulnerabilities
35	PFRDA	Pension Fund Regulatory and Development Authority
36	PFRDA TRACE	PFRDA - Tracking Reporting Analytics & Compliance e-Platform
37	PINTRA	PFRDA Intranet portal- Internal Digitalization
38	RFP	Request for Proposal
39	RPO	Recovery Point Objective
40	RTO	Recovery Time Objective
41	RTP	Real-Time Transport Protocol
42	SDD	System Design Document
43	SEBI	Securities and Exchange Board of India
44	SI	System Integrator
45	SLA	Service Level Agreement
46	SOC	Security Operations Centre
47	SOW	Statement of Work
48	SRS	System Requirement Specification
49	SSL	Secure Sockets Layer
50	STQC	Standardization Testing and Quality Certification (STQC)
51	TLS	Transport Layer Security
52	VPN	Virtual Private Network

3. Definitions

In this connection, the following terms shall be interpreted as indicated below:

1. **Annual Maintenance Contract (AMC)** - It would be the annual cost of maintenance of Software Solution/Service.
2. **Authority** - means the Pension Fund Regulatory and Development Authority (PFRDA), a Statutory Body established under the PFRDA Act, 2013.
3. **Bid** - means the written reply or submission of response to this RFP.
4. **Bidder** - means an eligible entity/firm submitting the Bid in response to this RFP.
5. **Contract** - means the agreement duly executed entered between PFRDA and the System Integrator, including all attachments and appendices thereto and all documents incorporated by reference therein.
6. **Go Live** - means implementation of complete solution as per requirements mentioned in this RFP.
7. **QCBS Award of contract** - means Bid scoring highest score based on QCBS method (Quality and Cost Based Selection) combining score of bidders giving weightage of 70:30 for technical and financial scores respectively.
8. **SI/System integrator** - means is the successful bidder who has been awarded the contract.
9. **Software Solution/Services/System/Project/e-PLATFORM/TRACE** – means All software products, services, scope of work and deliverables to be provided by a Bidder as described in the RFP and services ancillary to the development of the solution, such as installation, commissioning, integration with existing systems, provision of technical assistance, training, certifications, auditing, and other obligation of Service Provider as covered under the RFP.
10. **Total Cost of Ownership/Project Cost/TCO** - The price payable to SI over the entire period of Contract for the full and proper performance of its contractual obligations.

4. Notice Inviting Bids (NIB)

RFP Reference No: PFRDA/2024/TARCH/PFRDA-TRACE/01

RFP Name: Request For Proposal For Selection Of System Integrator(SI) For Design, Development, Implementation And Maintenance Of PFRDA-TRACE (PFRDA - Tracking Reporting Analytics & Compliance e-Platform)

Pursuant to this RFP, the Pension Fund Regulatory and Development Authority (PFRDA) invites prospective bidders to submit their bids for the implementation of digital platforms for undertaking its regulatory and supervisory functions of PFRDA ecosystem, as described below:

1. PFRDA-TRACE (PFRDA - Tracking Reporting Analytics & Compliance e-Platform)

PFRDA-TRACE (PFRDA - Tracking Reporting Analytics & Compliance e-Platform) will streamline interactions with its regulated entities, offering an e-PLATFORM for onboarding all existing intermediaries. The e-Platform features include but not limited to – submission of compliance data & reports, two-way communication, reminder alerts & notifications, reports, dashboards, workflow management. This initiative aims to enhance efficiency, ensure compliance, and provide a centralized repository of intermediary data & reports, including historic compliance records.

PFRDA-TRACE will also have comprehensive API layer for PFRDA which should also be able to send or receive reports/data from its intermediaries as required. PFRDA-TRACE Business Intelligence (BI) layer will offer Analytics and Reporting Tools for various purposes. This platform will empower PFRDA departments to conduct analyses on compliance, gain insights into the performance of PFRDA regulated & administered ecosystem and generate both regular and ad-hoc reports. Equipped with analytical capabilities, PFRDA-TRACE should ensure access to the insights necessary for effective supervision, regulatory policy development, research, and growth of the pension sector.

1. Interested bidders are requested to submit their proposals in accordance with the instructions provided in this Request for Proposals (RFP) document.
2. The purpose of PFRDA floating this RFP is to seek a detailed technical and financial proposal for procurement/development of an e-PLATFORM as desired in this RFP. The proposed e-PLATFORM must have seamlessly integration features and uniform look with PFRDA's other existing modules.
3. Interested Bidders are advised to carefully go through the entire RFP before submission of Bids, understand fully their eligibility and capability to undertake and execute the work.
4. Address for submission of Bids, contact details including email address for sending communications are given in ***Schedule of Events*** of this RFP.

5. Schedule of Events

Request For Proposal For Selection Of System Integrator(SI) For Design, Development, Implementation and Maintenance of PFRDA-TRACE (PFRDA - Tracking Reporting Analytics & Compliance E-Platform)

Name and Address of the Organization	Pension Fund Regulatory And Development Authority(PFRDA) B-14/A, Qutab Institutional Area, Chhatrapati Shivaji Bhavan, Katwaria Sarai, New Delhi-110016
RFP Ref. no.	RFP Reference No: PFRDA/2024/TARCH/PFRDA-TRACE/01
Bid processing Fee	Rs. 25,000/- (Rupees Twenty-five thousand only) plus GST @18% as applicable that is Rs 29,500 (Twenty-nine thousand and five hundred only). Bid processing fee to be transferred electronically to PFRDA designated Bank Account or in the form of Account payee demand draft in favour of PFRDA, New Delhi. Details of bank accounts are given in this table. ***Note:*** Bidders who have submitted bid proposals against EOI for TARCH project Ref no.: PFRDA/2022-23/IT/02 issued on 27 June 2022 and not submitted bid for RFP ref. no.: PFRDA/2023/TARCH/PINTRA/01 issued on 4th July 2023 are exempted from submitting Bid Processing fee.
Earnest Money Deposit (EMD)	Rs 1,20,00,000 (Rupees One Crore Twenty Lakhs only) EMD should be submitted by the bidders in the form of a Performance Bank Guarantee (BG)/Fixed Deposit Receipt - issued by a Scheduled Commercial bank lien marked in favour of PFRDA /Online Payment in the designated bank account of PFRDA. The EMD submitted in the form of bank guarantee/Fixed deposit receipt should be valid up to at least 180 days from the bid submission end date.
Performance Security	10% of the /Total Cost of Ownership (TCO)/ Total Contract Value as quoted in Financial bid. Performance Security to be submitted by the Successful Bidder in the form of a Performance Bank Guarantee (BG) which should be valid at least up to 180 days from the date of completion of the contract. The successful bidder shall extend the Performance Security depending on the extension of the Contract period. Performance security may also be submitted in the form of Fixed Deposit Receipt - issued by a Scheduled Commercial

	bank lien marked in favour of PFRDA and should be valid at least up to 180 days from the date of completion of the contract. The successful bidder shall extend the fixed deposit depending on the extension of the Contract period.
Date of Publishing the RFP	*31st January 2024*
Last date of submission of pre-bid queries	*9th February 2024 up to 1800 Hours*
Email id on which pre-bid queries to be sent	itprojects-pfrda@pfrda.org.in
Date, Time, and Venue of Pre-bid Meeting	*15th February 2024* Venue & Time to be notified on PFRDA website (https://www.pfrda.org.in) and Central procurement portal CPPP (https://eprocure.gov.in/epublish/app)
Project Head	Shri. Akhilesh Kumar - Chief General Manager In charge - TRACE
Nodal Officer details for IEM Co-ordination of the RFP	Shri Girraj Yadav, Assistant Manager, PFRDA
Bid Submission Start Date	*31st January 2024*
Bid Submission End Date and Time	*11th March 2024 up to 1500 Hours*
Address for Submission of RFP Document (through speed post/registered post/in person) to be submitted in the tender box located at the reception of PFRDA office premises	To, Chief General Manager In charge- PFRDA-TRACE Chhatrapati Shivaji Bhavan, B-14/A, Qutab Institutional Area, Katwaria Sarai, New Delhi- 110016
Technical Bid Opening Date and Time	*11th March 2024 at 1530 Hours*
Presentation by the bidders	To be communicated to the eligible bidders at the later stage.
Financial bid Opening Date and Time	To be communicated to the technically qualified bidders at the later stage.
Issue of Letter of Intent (LOI) to the successful bidder	After approval from the Competent Authority
Contract Finalization and award	After approval of the Competent Authority and on receipt of required Performance Security & Non-Disclosure Agreement (NDA)
Bid Validity	180 Days from the bid submission end date

PFRDA Bank Account details	Beneficiary Name – Pension Fund Regulatory and Development Authority Bank Name - Indian Overseas Bank Branch Name – F-75, Poorvi Marg, Vasant Vihar Branch, New Delhi-110057 Account No – 159901000000855 IFS Code – IOBA0001599
PFRDA GSTIN no.	07AAALP0291L1ZU

6. About PFRDA

1. Pension Fund Regulatory and Development Authority is a statutory body, which operates within the legal framework of PFRDA Act, 2013, with an objective to promote old age income security by establishing, developing, and regulating pension funds, to protect the interests of subscribers to schemes of pension funds and for matters connected therewith or incidental thereto.
2. The Pension Fund Regulatory and Development Authority Act (23 of 2013) ("PFRDA Act/the Act") was notified on 1 February 2014 in the Gazette of India. PFRDA is regulating the National Pension System ("NPS"), subscribed by the employees of Govt. of India, State Governments and by employees of private institutions/organisations & unorganised sectors. Later, in the year 2015, a government-backed minimum guarantee pension scheme named "Atal Pension Yojana" ("APY"), primarily targeted at the unorganised sector, was launched by the Government of India on 09 May 2015 and the administration of the scheme has been handed over to PFRDA.
3. PFRDA is responsible for regulation & supervision of various intermediaries such as Central Record Keeping Agencies (CRAs), Pension Funds (PFs), Point of Presence (POPs), Custodian, Trustee Bank, etc. PFRDA has a significant role to play in safeguarding the interest of the subscribers. It regulates the manner in which each intermediary function under the NPS architecture so as to ensure fair play for subscribers. It also ensures that all stakeholders/intermediaries comply with PFRDA Act and Rules /Guidelines/Regulations/Circulars issued by PFRDA Act from time to time. The duties, roles and responsibilities of the Authority are as per Sec 14 of PFRDA Act, 2013.
4. The Authority consists of the following Members, namely:
    a. Chairperson.
    b. Three whole-time members.
    c. Three part-time members.
5. The following table gives an insight about PFRDA employees & future projections:

Table 7.1: Existing internal PFRDA user base and future projections

Sr. No.	Departments	Current Employee Strength	Users in 5 Years
1	Regulation	Executive Director – 3 Chief General Manager – 2 General Manager – 1 Deputy General Manager - 1 Assistant General Manager – 2 Manager – 3 Assistant Manager - 2	24
2	Supervision	Executive Director – 3 Chief General Manager - 3 General Manager – 1 Deputy General Manager - 2 Assistant General Manager – 5 Manager - 5 Assistant Manager – 8	49
3	Promotion & Development - APY & NPS	Executive Director -1 Chief General Manager – 2 Deputy General Manager - 1 Assistant General Manager - 4 Manager - 1 Assistant Manager – 5 Management Executive – 2	23
4	Communication & Media, Financial Literacy, Secretariats, Regulation Review Secretariat, Pension Sanchay, NCFE, SEPF, Helpdesk - APY/NPS, Training, Annual Report, FSLRC, FSDC, IOPS, Inter Regulatory Matters,	Executive Director – 2 Chief General Manager – 1 General Manager – 1 Assistant General Manager – 4 Manager – 1 Assistant Manager – 5 Junior Assistant - 1	20
5	HR & Admin, Rajbhasha	Executive Director -2 Chief General Manager – 2 Deputy General Manager - 1 Assistant General Manager -2	12

		Assistant Manager – 4	
6	Finance and Accounts	Executive Director - 1	6
		General Manager - 1	
		Manager -1	
		Assistant Manager -3	
7	IT, Fintech & Data Analytics, TARCH	Executive Director – 2	20
		Chief General Manager – 2	
		General Manager – 1	
		Assistant General Manager – 1	
		Manager – 3	
		Assistant Manager – 6	
		IT Project Manager -1	
8	Legal and Internal Audit, RTI & PQ, Enforcement & Adjudication, Investigation, Vigilance, Grievance Cell, Ombudsman, Public Grievance Portal, CPENGRAM	Executive Director – 2	20
		Chief General Manager – 3	
		General Manager – 1	
		Deputy General Manager – 2	
		Assistant General Manager – 2	
		Manager – 2	
		Assistant Manager – 6	
		Legal Consultant - 1	
9	Policy Research, Systemic Risk Management, Market Watch, Pension Bulletin.	Executive Director – 1	12
		General Manager -1	
		Assistant Manager – 3	
10	Innovation Hub	NA	3
11	Investigation and Surveillance	NA	2
12	**Total**	92 (Unique Number)	216

Note-1: *The total at Row 12, Column 3 is arrived at by counting the unique individual users only to avoid repetition in case the same user is present in two different departments. Staff Car Driver is not included.*
Note-2: *Chairperson & WTMs are not included and they may be suitably included.*

Note – 3: *The above is as on information. However, SI should size the solution in such a manner that there is no over-sizing of the solution or under-sizing of the requirements at the requirement gathering stage.*

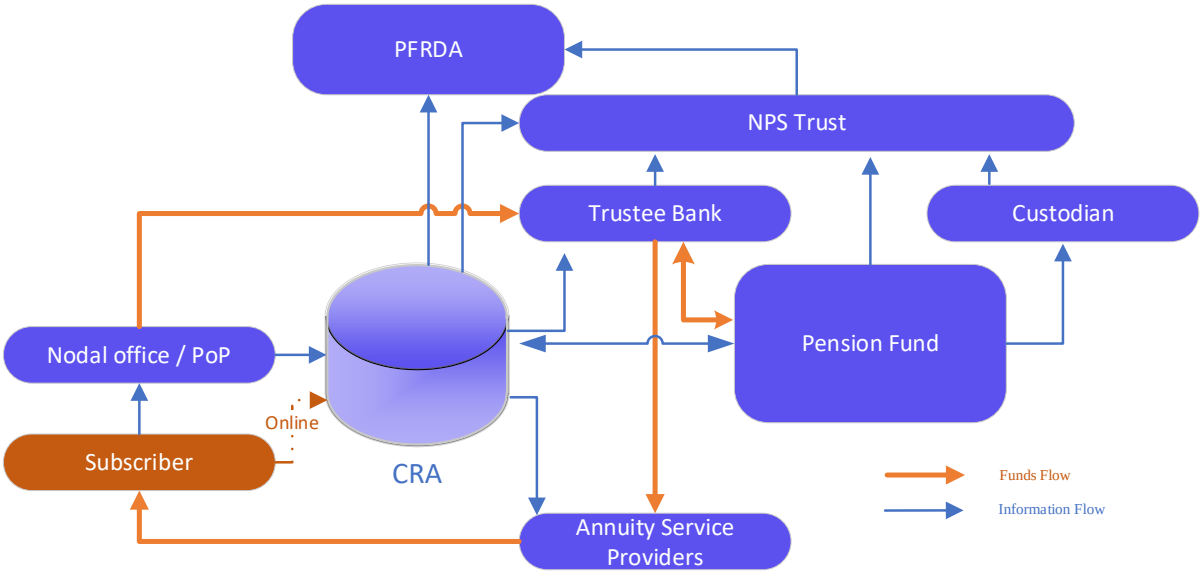


Figure 7.1: NPS Architecture

Following are the intermediaries which are part of NPS architecture.

1. **Point of Presence (POP)-** POPs are the first point of contact and act as an interface between the subscriber and NPS architecture. The primary responsibility of the POPs is to act as a distribution channel of NPS and assist prospective subscribers in opening of NPS account and collect subscriber's contribution and remit the same to Trustee Bank. POPs also provide other ancillary services to the subscribers during maintenance and exit of the subscribers from NPS.
2. **Central Record Keeping Agency (CRA) –** CRAs are registered by PFRDA to perform the functions of recordkeeping, accounting, and administration for subscribers. The CRA is responsible for receiving instructions from PoPs and subscribers etc. through CRA web system, transmitting such instructions to the appointed Trustee Bank and Pension Fund to act accordingly. The CRA monitors subscriber contributions and instructions and transmits information to the Trustee Bank and relevant Pension Fund on a regular basis. The CRA provides periodic, consolidated PRAN statements to each subscriber and has hosted the eNPS online platform on behalf of NPS Trust.
3. **Pension Fund (PF) -** Pension Funds manages the retirement savings of subscribers under the NPS. PFs use their secure access codes to confirm receipt of netted assets and instructions regarding fund allocation, confirm allocation of funds and communicate the NAV of each scheme to CRA(s) on a regular basis.
4. **National Pension System Trust (NPST) -** It is established by PFRDA under the provisions of the Indian Trusts Act of 1882 for taking care of the assets and funds under the NPS in the best interest of the subscribers. NPS Trust is the registered owner of all assets under the NPS architecture which is held for the benefit of the subscribers of the NPS. The securities are purchased by Pension Funds on behalf of, and in the name of the NPS Trust, however individual NPS subscriber remains the beneficial owner of the securities, assets, and funds.

5. **Annuity Service Provider (ASP) -** ASPs are responsible for delivering a regular pension to the subscriber for the rest of his/her life. On receipt of specified sum along with personal and banking information details of subscriber from CRA(s), the ASP would use its access codes to confirm receipt. ASP would then begin payments of annuities to the subscriber.
6. **Custodian -** Custodian means an entity which has been granted a certificate of registration under sub-section (3) of section 27 of the Act by the Authority as a Custodian of securities for the purpose of providing custodial and depository participant services for the pension schemes regulated by the Authority.
7. **Trustee Bank -** The Trustee Bank is registered by PFRDA for providing banking services to the NPS architecture. The Trustee Bank receives funds from various nodal offices/PoPs, reconciles the funds received with the subscriber details provided by CRA, transfers funds to PFs and Annuity Service Providers (ASPs) based on instruction given by CRA.

The following table provides information about the current scenario and approximate number of PFRDA stakeholders/intermediaries.

Table 7.2: Stakeholders/Intermediaries envisaged for this project (indicative).

S. No	Stakeholders/Intermediaries	Approximate Number of entities	Approximate no. of Users
1	NPS Trust	1	3
2	Pension funds	11	33
3	CRA	3	12
4	Custodian	1	3
5	Trustee bank	1	3
6	Points of Presence	350-400	800
7	Annuity Service Providers	15	30
8	Retirement advisers	150	150

Note : *The above is as on information. However, SI should size the solution in such a manner that there is no over-sizing of the solution or under-sizing of the requirements at the requirement gathering stage.*

7. Objective

The primary goal of this project is to establish a comprehensive workflow management, reporting platform, dashboard layer with Business Intelligence (BI), with data management system for the compliance management framework. The application to manage timely compliance of data submissions, data retrieval, storage, validation, and execution of various data analytics procedures. Additionally, the project aims to streamline and automate stakeholders/intermediaries' interactions in accordance with the existing provisions of PFRDA Act, Rules, and Regulations.

This initiative anticipates a substantial reduction in manual processes, including document handling, data entry, processing, and long-term data storage by the implementation of an integrated software solution. The envisioned solution is expected to facilitate efficient data processing, analysis, reporting, retrieval, management, and reorganization through collaboration & automated workflows.

Furthermore, the system's design should ensure compatibility with a broad range of web browsers, operating systems and devices including desktop computers, laptops, and mobile devices while also exhibiting responsive behaviour.

8. Current Status of IT landscape

PFRDA's own assessment of current technology landscape related to present work is that most of the operations are performed manually and digitization is partial.

PFRDA envisages a turn-key project Technology Architecture (TARCH) comprising of automation of its internal processes, Regulatory and Supervisory framework, Data Analytics and PFRDA website revamp. The TARCH project will be executed through multiple RFPs. This RFP is issued in respect of automation of its compliance and regulatory functions with various analysis based on the data retrieved and reports submitted by the intermediaries.

1. PFRDA is in the process of developing another IT system known as PINTRA project as currently majority of its activities in HR, Administration, Finance & Accounts, IT, Legal are manually executed, utilizing tools such as MS Word, Excel spreadsheets, and email. This project aims to create an Intranet portal for internal digitalization, encompassing modules for HRMS, Finance, Administration, Legal, IT management and Incident management. Notably, the PINTRA project will be hosted on a cloud-based platform.
2. PFRDA is using e-office, a software solution provided by NIC, has an e-File and Collaborative tool for Knowledge Management module that is used mainly for file management and Document Management. e-office will be continued as File Management System.
3. PFRDA website (https://pfrda.org.in) and PFRDA microsite (https://pensionsanchay.org.in) are hosted on the NIC Cloud. PFRDA has a portal for

Retirement Advisers named as RP portal (https://reap.pfrda.org.in/pfrdareap/). RP portal and e-office are hosted on NIC data Centre.

9. Scope of Work - PFRDA TRACE

SI is expected to undertake a comprehensive project i.e., a software solution to meet the requirements of Pension Fund Regulatory and Development Authority (PFRDA) as provided in this RFP. Bidders shall diligently study this RFP and all related documents mentioned herein to gain a thorough understanding of the project's objectives and requirements which are given in brief below:

PFRDA recognizes the need for a modern system like PFRDA-TRACE (PFRDA - Tracking Reporting Analytics & Compliance E-Platform). This solution is needed to modernize and streamline the regulatory, supervisory and data management processes, enabling seamless interactions with the intermediaries, ensuring compliance, and harnessing the power of data-driven supervision. PFRDA-TRACE would serve as a digital gateway for intermediaries to submit compliance reports & data, also acts as a robust data warehouse and analytics platform. This would empower PFRDA to proactively monitor, supervise and govern its regulated entities.

1. PFRDA - Tracking Reporting Analytics & Compliance e-Platform

(Supervisory and Regulatory Compliance Reporting Platform for Intermediaries)

PFRDA regulated entities include NPS Trust, Central Record Keeping Agencies (CRAs), Points of Presence (PoPs), Pension Funds (PFs), Trustee Bank (TB), Custodian, Retirement Adviser (RAs) and there are some other stakeholders who are integral to the NPS System like Govt. Nodal Offices, Annuity Service Providers (ASPs) etc. In order to enable seamless interactions with the intermediaries and stakeholders, an online e-PLATFORM has been envisaged to provide a common interface for all intermediaries to submit regulation-related reports, supervisory compliance data and other related information to PFRDA for offsite monitoring, surveillance, and compliance-related activities.

This digital solution for Supervisory and Regulatory Compliance Reporting Platform for Intermediaries envisaged and named as **PFRDA-TRACE (PFRDA - Tracking Reporting Analytics & Compliance e-Platform).** This system will enhance the efficiency and effectiveness of monitoring and ensuring timely compliance of its regulatory, supervisory, and administrative framework. As part of this initiative, PFRDA aims to introduce an online e-PLATFORM for its stakeholders with the functionalities such as onboarding of existing intermediaries for accessing the envisaged platform, compliance submission by intermediaries, monitoring of regulatory & supervisory functions. The system will check for conformance with the Regulatory Guidelines and will also provide alerts for deviations/mismatches, imminent deadlines, and any delays in the submission of data/information/report required for supervision. It shall also include workflows for various PFRDA departments to review and accept, reject, or identify deviations in compliance-related information submitted by intermediaries and track

them for closure. Master information about the intermediary, e.g., shareholding pattern, key management personnel details, Compliance Officer details, etc. shall also be included along with historic information about exceptions in compliance, submissions, changes etc.

The e-PLATFORM has to be designed with rule-based intelligence and should be capable to send reminders in the form of emails, generate alerts based on inbuilt rules, which can be objectively measured. The system should also have the capability to communicate remarks to the respective intermediary with respect to non-compliance or any other variation observed in the report and accept the resubmission/replies on the observations for process completion. The reports, compliances and data submitted by Intermediaries should be able to be validated by PFRDA.

Key features and functionalities of the PFRDA-TRACE platform includes but are not limited to:

1. Onboarding for access to the e-Platform: Onboarding of registered intermediaries for accessing the envisaged platform easily.
2. Compliance Monitoring**:** The proposed solution should automate the compliance monitoring process for PFRDA regulated entities, ensuring that they adhere to regulatory requirements, reducing the likelihood of non-compliance and regulatory violations.
3. Efficient Communication: The proposed solution should be able to enable efficient communication between PFRDA and its regulated entities, reducing delays and facilitating faster issue resolution, promoting transparency and cooperation.
4. Integration with communication channels: The e-Platform seamlessly integrates with SMS and email gateways to enable secure transactions and efficient communication.
5. Report Submission: Intermediaries can upload supervisory and regulatory reports for different specified periods such as daily, weekly, monthly, quarterly, half-yearly, annually and for any other periodicity defined as per the requirement.
6. Review and Deviation Handling: The platform enables PFRDA to review, accept, reject, or identify deviations in the submissions made by intermediaries. This ensures that the reports adhere to regulatory standards.
7. Dashboards: Dashboards to provide a comprehensive view of adherence to regulatory requirements, allowing for better oversight of compliance of intermediaries by PFRDA.
8. Notifications and Alerts: PFRDA-TRACE to generate intelligent notifications and alerts for various actions – such as submission deadlines, exceptions in submissions, pending submissions and any delays.
9. Custom/Intelligent Web Form Design and Configurable Workflows: PFRDA Users can design new forms and configure workflows to accommodate changing regulatory requirements and reporting standards.
10. Scalability and Interoperability: The platform should be designed to scale with growing requirements and can seamlessly integrate with other systems. It should be flexible and adaptable to meet evolving needs.

11. Rule-Based Compliance: The platform is expected to use rule-based checks to assess both quantitative and qualitative compliance, generating reports based on these checks.
12. Authenticated Reporting: The platform is required to provide an authenticated interface for intermediaries within PFRDA Architecture. It includes a maker/checker facility for data validation and integrates with digital signature certificates and e-sign technology to ensure the security and authenticity of submissions.
13. User authentication: The Solution Integrator (SI) should enhance the security of the designated group of users responsible for data feeding. The scope of this security measure should exclude dashboard users to ensure focused protection for sensitive data entry operations.

An approximate count of the report submission users is around 750 today. Expected concurrent users will be One Hundred (100) (approximately). Over the time of 6 years the number could grow up to 10-20 %. The user groups are – POPs, Pension Funds, Trustee bank, Annuity Service Providers (ASPs), CRAs, Custodian, Retirement Advisors (individual & non individual).

Approximate report counts & Sizing: In the current operational landscape, Pension Fund Regulatory and Development Authority (PFRDA) relies on a multitude of reports distributed across its diverse departments to address various functional requirements. The approximate report counts, and size presented herein serves as an indicative representation in the following tables:

S. no	Category of report	Approximate Count*
1	Large 10 - 20 mb	13
2	Medium 5 - 10 mb	14
3	Small <= 5 mb	197

* The report count is based on each individual Excel or PDF file; the number of worksheets within these files is not considered.

Compliance cum Data Reports	Approximate Count*
PDF	62
Total No of Sheets in Excel	162

Note: The number of reports mentioned above in both the tables are indicative. The implementation/digitalization will depend on the creation of web forms, potential variation in the data architecture and frequency of submissions.

PFRDA-TRACE to also feature a Business Intelligence (BI) layer to be built. It should manage analytics and reporting for supervision, regulatory policy formation, research, promotion & development-related activities to meet the objectives of PFRDA.

The key components and features of the data & analytics module within PFRDA-TRACE encompass the following:

1. **Report Automation**: It should automate the generation of standard reports and exceptions for surveillance and market insights, as well as reports needed for regulatory policy formulation, promotion, and development activities.
2. **Data Analytics Tools**: It should be equipped with analysis capabilities and data visualization tools.
3. **BI and Reporting:** The system will automate the generation of multiple MIS and standard compliance reports, delivering desired frequency via the data and analytics e-Platform or email. Users are empowered to generate ad-hoc reports to meet their unique requirements. Customized and standard dashboards are readily available, allowing departments to uncover insights tailored to their needs.
    a. **Data Visualization Tools:** BI-Layer should offer a wide range of data visualization tools, including charts, graphs, dashboards, and heatmaps for presenting data in a user-friendly format.
    b. **Scheduled Reports:** Users should be able to schedule automated report generation and delivery based on predefined intervals.
4. **Dashboard:** PFRDA-TRACE encompasses an Analytics cum Monitoring Platform, for enhancing the Pension Fund Regulatory and Development Authority's (PFRDA) data-driven capabilities. Within this platform, the Dashboard component stands as a crucial segment, providing a comprehensive panoramic view of intermediary activities and department-specific functionalities, covering research, supervisory, regulatory, promotion & development, as well as training & development initiatives. This Dashboard serves as a dynamic and centralized hub, facilitating real-time insights and data visualization, enabling PFRDA to make informed decisions, monitor activities, and drive strategic initiatives with precision and efficiency across all facets of its operations.
5. **Data Warehousing:** The platform to include a robust data warehousing capability for aggregating data collected.
6. **API Management Layer:** An API management layer is required for developing, designing, monitoring, testing, securing, and analysing various APIs for PFRDA. This tool to ensure that API as required by PFRDA could be developed without much dependency/development effort.
7. **Data Export and Sharing:** System should be capable of data export & sharing as per the details as mentioned as below:
    a. **Data Export**: The system should allow authorized users to export reports and data in various formats, including PDF, Excel, and CSV.

b. **Data Sharing**: Users should be able to share reports and dashboards with authorized stakeholders.

8. **Embedding**: The BI-LAYER should support the embedding of reports and dashboards in external applications or websites.
9. **Data Retention:** The proposed solution should be capable of long-term data retention. PFRDA should be able to store historical data and maintain data for compliance, auditing, or future analysis without significant costs.
10. **Automated Reporting and Alerts:** The proposed solution should be able to automate the creation of reports and alerts for PFRDA based on predefined criteria, reducing the manual effort required.
11. **Automation:** The proposed solution should be able to automate various compliance tasks, reducing the need for manual intervention and minimizing errors.
12. **Data Visualization:** The proposed solution should be able to create visualizations that can help PFRDA understand complex data sets, for more informed decision-making.
13. **Enhanced Supervision:** The solution should enable PFRDA to track the performance of PFRDA regulated entities, evaluate their risk exposure, and intervene when necessary.
14. **Improve Efficiency:** This platform should automate and streamline regulatory and supervisory processes, reducing the administrative burden.
15. **Monitoring:** This platform should enable monitoring of PFRDA regulated & administered ecosystem, allowing PFRDA to detect potential issues and anomalies as they occur, in addition to periodic reporting.
16. **Scalability:** The proposed solution should be highly scalable. PFRDA should be able to scale its storage and processing capabilities horizontally as the data volume grows. This scalability should ensure that it can accommodate increasing data needs without major infrastructure overhauls.
17. **Simplified Compliance:** The proposed solution should be able to help the regulated entities benefit from a unified platform that streamlines the process of regulatory compliance, making it easier to meet reporting requirements.
18. **Standardization and Consistency:** The proposed solution should promote standardization and consistency in processes and data collection, ensuring uniformity in reporting.
19. **Transparency:** The proposed solution should be able to help the regulated entities to access a transparent regulatory framework, with clear guidelines and reporting processes.
20. **Ad-Hoc reporting** – The system should provide ad-hoc reporting feature for dynamic and on-demand process to empower PFRDA users to create customized reports and analyses as needed.
21. **Ease of use:** The user of PFRDA will have a seamless access for all the modules of PFRDA-TRACE.

22. **Data Security and Governance:** The system will have strong data security features and tools to avoid any data leakage and unauthorised access and maintain confidentiality of data/information between intermediaries. Data security is upheld by granting role-based access to business teams for curated data, as well as reports. Data quality tools will play a pivotal role in delivering cleansed and standardized data across the layers. The proposed solution should be capable of implementing access control and governance policies.

PFRDA-TRACE holds paramount importance in increasing the efficacy of PFRDA's regulatory, supervisory, and administrative operations and discharge its functions flowing from the PFRDA Act, 2013. Foremost among the project's objectives is the facilitation of a conducive environment for Ease of Doing Business (EODB), ensuring prompt compliance and adherence to regulatory standards. Moreover, this initiative is pivotal in harnessing analytical capabilities to support the monitoring and oversight of PFRDA administered ecosystem, take proactive measures for risk mitigation. The achievement of an improved EODB environment remains a paramount outcome of this endeavour, aligning with the broader goals of enhanced governance and compliance within PFRDA.

Indicative detailed functional requirements about PFRDA-TRACE are provided in ***Schedule II***. Technical Details are provided in ***Schedule III***.

2. Comprehensive project outline

The successful Bidder is expected to undertake a comprehensive project for the provision of a software solution to meet the requirements of the Pension Fund Regulatory and Development Authority (PFRDA) as mentioned in this document. Bidder shall diligently study this RFP to gain a thorough understanding of the project's objectives and requirements. Broad Project Execution Steps covering the following broad steps during the execution of the project:

1. Start-Off/Kick-off Meeting
2. Requirement Gathering (As-Is & To-Be Analysis)
3. Documentation: BRD, FRS, SRS, Design Guidelines, SDD, etc.
4. Infrastructure for Dev-Ops
5. Development: Customization, Configuration, 3rd party Integration
6. Deployment
7. Testing
8. Implementation
9. Post Implementation support
10. Training
11. Licensing
12. Security Audit and Vulnerability Assessment and Penetration Testing (VAPT)
13. Setup Helpdesk

14. Stabilization phase
15. Go-Live
16. Post Implementation Support
17. Warranty
18. AMC Support
19. Change Management during AMC phase

a) Start-Off/Kick-off Meeting

Start-off is the first activity after award of the project to SI, focusing on the project objective, milestones, resource roles and responsibility.

b) Requirement Gathering (As-Is & To-Be Analysis)

Conduct a thorough study of existing processes and come up with a 'As-Is' & 'To-Be' processes. It is preferred that the project would be run on a collaboration tool.

SI should submit a project charter, project plan with sprint planning, final team structure.

As-Is Analysis

1. SI is expected to get detailed understanding of the existing processes, systems, workflows including manual operations.
2. SI needs to understand the scope of the integrated solution.

To-Be Analysis

1. SI is expected to propose a seamless integrated solution with uniform User interfaces.
2. The architecture should be loose coupled and based on open standards to support scalability and integration to existing and futuristic modules.
3. SI shall prepare & submit an Integrated Project Plan for the entire project that covers detailed tasks including optimized data architecture, Business Process Reengineering for reports as analysed during the project tenure, which are intended to be performed as part of the project along with the scope and duration of each of the activity.
4. Any other relevant and connected activity as per enterprise best practices.

c) Documentation: BRD, FRS, SRS, Design Guidelines, SDD, etc.

Create and prepare detailed documentation, including Business Requirement Document (BRD), Functional Requirement Specification (FRS), Design guidelines with wireframe and UI & UX Specifications, System Requirement Specification (SRS). These documents to be prepared by highly experienced professionals in cognizance to the subject matter experts chosen by SI for the project.

1. SI shall be entirely responsible for architecture of the system implemented to satisfy all features, functions, performance including the security and shall ensure that the Systems design should adhere to the industry wide best practices and support futuristic integration and scalability.
2. Deployment and Configuration Documentation: Detailed instructions for deploying the software solution, configuring the environment, setting up databases, and any other necessary system configurations.
3. Detailed implementation schedule (module-wise) for entire solution within the timelines specified in the RFP must be prepared and submitted.
4. SI is required to submit fortnightly status reports showing progress against plan.
5. SI is required to maintain Software version management and software documentation management reflecting features and functionality of the solution.
6. Any changes introduced in the solution by way of redesigning formats/workflow/code level changes, etc. needs to be documented and submitted.
7. User Manuals and Training Materials: Documents that provide instructions and guidelines on how to use the software solution effectively. They may include user guides, FAQs, video tutorials, and training materials to facilitate user adoption and minimize support requests.
8. SI is required to provide suitable exit plan including cloud port out plan and Business Continuity Planning (BCP) applicable to the proposed solution.

d) Infrastructure for Dev-Ops

1. SI must arrange for supply of virtual hardware which ensures a standardised IT environment at the GCC or VPC from MeitY empanelled CSP, as per the latest cloud adoption guidelines stipulated for the purpose of development & operations.
2. Bidders are expected to provide details of requirements in the Bill of Material (BOM) attached as ***Annexure- XVIII***
3. Cloud Infrastructure Procurement & Management: Estimate and procure suitable cloud resources, specifically a Government Community Cloud (GCC) or Virtual Private Cloud (VPC) of at least tier III, with Disaster Recovery (DR) Centre. Bidder to ensure that all cloud services originate from a MeitY empanelled service provider. The solution should be accessible over the internet, ensuring access from anywhere while complying with Cloud adoption guidelines issued by Government authorities.
4. SI should propose and develop a tailored IT solution using one of the following approaches or a hybrid approach: a fully custom bespoke system designed from the ground up, a hybrid system that combines bespoke development with *'Enterprise grade'* Commercial Off-The-Shelf (COTS) or *'Enterprise grade'* Modified Off-The-Shelf (MOTS) products to create an integrated solution, or a complete *'Enterprise grade'* COTS/MOTS system built entirely upon commercially available products. SI's choice among these development approaches should be informed by the project's specific requirements and alignment with efficiency and effectiveness objectives.

5. For any *'Enterprise grade'* COTS/MOTS product implemented SI should ensure that the OEM of the proposed Platform/product has reviewed and certified all the Customizations/Configurations/Third (3rd) party integration before deployment at PFRDA. Such OEM Certification to be submitted to PFRDA before signing off the SRS document. If COTS product is proposed by bidder, it should have its customization inventory available.

e) Development: Customization, Configuration, 3rd party Integration

1. Post finalization and sign-off of the documents by PFRDA, SI is expected to start with the design and development of the application which will include incorporation of the proposed solutions, Customizations, Configurations, third (3rd) party integrations, development as required.
2. The development process should follow an agile methodology, allowing for iterative development and frequent feedback sessions with stakeholders.
3. To ensure robust architecture, code quality and best practices, PFRDA may interact with the development team and conduct regular code reviews and identify any potential vulnerabilities or performance bottlenecks.
4. Compliance with relevant coding and security standards, such as OWASP (Open Web Application Security Project), should be ensured throughout the development process.
5. SI should provide proper documentation for developers, including Application programming Interface (API) documentation, SDKs (Software Development Kits) and code samples to facilitate integration with third-party systems or future enhancements.
6. The development team should adhere to secure coding practices, including input validation, output encoding, and protection against common security vulnerabilities like SQL injection and cross-site scripting (XSS).
7. Code documentation should be maintained, including comments within the codebase and high-level documentation explaining the logic and functionality of key components.
8. Solution may preferably be made by use of Open-source software with Enterprise support. SI shall ensure that full support is provided from the respective OEM. Further, SI shall provide a list of all such open-source software/tools with Enterprise support being used in the platform.
9. Solution shall be modular with a clear separation of concerns at the data storage, service, and the API layer. The adoption of open standards shall work towards singular goal of interoperability which would ensure that all third-party interfaces are fully interoperable without any affinity to platforms, programming languages and network technologies.
10. Development of the application will be carried out at SI's development Centre or SI's premises.

11. SI must ensure that granularity is built in the solutions, sub-modules, and individual functionalities so that these functionalities can be enabled or disabled through administrator as per the requirements.
12. SI is expected to follow Secure Coding standards for application development.
13. SI is expected to ensure complete confidentiality and security of PFRDA's data.
14. SI should facilitate PFRDA or any of its authorized representatives to carry out audit at their development centres to check the progress of the project at any point of time.
15. The design and development of the comprehensive, structured, and integrated software solution shall be delivered including those indicative features & directives detailed/outlined further in Schedule II of this RFP.

    Note - The entire application should be developed in strict adherence to Indian IT standards for user interface (UI), user experience (UX), privacy and security, as well as in compliance with all applicable laws and regulations of India in force at the time of development and deployment.

    Example - GIGW 3.0, SO/IEC 27001, OWASP Top Ten, WCAG (Web Content Accessibility Guidelines), Regulators such as RBI (Reserve Bank of India), SEBI and IRDAI Guidelines for IT system design, Data Protection Laws (e.g., DPDP act/Indian Data Protection Law), UI/UX Design Principles, Secure Coding Practices, IT Act 2000, and as per the latest Legal and Regulatory Updates in the country.

f) Deployment

1. During deployment, SI is responsible to check for the latest version update for any Major/Minor technology component. Based on the suggestion from SI, the Change Control Board of the project will make the decision whether to retain the latest version, denoted as 'N,' or the immediately preceding version, 'N-1', for production & other environments of the project. In no scenario the versions should be beyond 'N-1'.
2. Staging, development, and production environment to be kept & managed by SI separately.
3. Continuous integration and continuous deployment (CI/CD) practices should be implemented to automate the build, testing, and deployment processes, ensuring rapid and reliable software delivery.

g) Testing

1. SI shall provide details of tests being carried out during the implementation (e.g., including unit tests, system integration tests, regression tests and user acceptance test).
2. SI shall work in a manner to satisfy all the testing requirements and adhere to the testing strategy outlined. SI must ensure deployment of necessary resources and tools during the testing phases. SI is responsible to take remedial action based on outcome of the tests.
3. SI is to create the test strategy document that defines the requirements and configurations of the solution, determine the tools and methods used to check that the

application responds correctly, determine how and when the test will be performed. The test strategy document may guide the project team through the implementation to ensure that planning and conducting testing activities in the various phases of integrated solution implementation are proper.

4. SI should establish proper test environments that closely resemble the production environment, including the necessary infrastructure and dependencies for comprehensive integration, system, and automation testing.
5. The various testing phases are as follows:

a) Development and Functional testing

1. Post development and customization of the solution, SI shall conduct tests to demonstrate the readiness of the system which meets all the requirement specifications (functional and non-functional) as brought out in this RFP.
2. Based on these tests, a report shall be submitted by the System Integrator for review and approval by PFRDA.
3. SI to ensure that the test results reflect the business requirements as defined in this RFP.

b) Integration, System and Automation testing

1. The purpose of the integration test is to execute the integrated components and analyse the results that are important for the functional verification of the system.
2. Integration testing shall be accomplished through the execution of predefined business flows or scenarios, that emulate how the system will run the processes. The integration tests shall reflect that the solution is complete and will perform the business processes of PFRDA.
3. SI shall submit a report capturing the results of successful testing.

c) Load, Stress, Performance and Regression testing

1. Once the system integration testing of the configured and customized solution has been conducted successfully, Load, Performance, Scalability, and Regression testing would be conducted prior to Go- Live.
2. SI is required to perform Load and Stress Testing to demonstrate the ability of the application and underlying infrastructure to perform without degradation when under maximum traffic load carrying conditions.
3. After successfully completing above stated testing and its clearance with PFRDA, the solution would then be considered as ready for Go-Live.
4. SI is required to submit a report demonstrating successful completion of testing.

d) User acceptance testing (UAT)

1. SI will develop procedure for UAT along with PFRDA project management team for PFRDA’s approval, prior to start of the UAT phase. The purpose of this

acceptance is to ensure conformance to the required operations, response times, and integrity of the software after installation, and to eliminate any operational bugs.

2. A critical criterion for UAT would be the validation and conformance of solution in terms of details captured in the technical design document.
3. UAT shall be carried out before Go-Live at site as per approved procedure and the test reports shall be signed off.
4. At the satisfactory conclusion of these acceptance tests, the implementation of the software shall be considered complete for Go-live. The UAT must carry out at PFRDA location.
5. SI is required to submit a report demonstrating successful completion of testing.
6. Any deviations/discrepancies/errors observed during the testing phase will have to be resolved by SI. Any exceptions will have to be documented and signed off by PFRDA.
7. SI is expected to make all necessary modifications to the solution, customizations, interfaces, etc., if there are performance issues or errors identified during testing, it will have to be rectified and subsequent patches/versions will also have to be tested.
8. SI shall set up and maintain a test server, install the base/customized application, or developed software and parameterize and upload test data into the test server. SI shall also provide the test scenarios and the test cases for review to PFRDA.
9. UAT will be firstly done from department/offices of PFRDA and later by a third party if PFRDA so desires, expenditure for engaging a Third (3rd) party for UAT, if any will be borne by PFRDA.
10. SI shall be responsible for maintaining appropriate program change control and version control for all the modifications/enhancements carried out during the implementation/ testing phases.SI is expected to provide details of the testing strategy, testing approach, teams responsible for the entire activity (implementation/testing phases).

h) Data Migration

1. SI to provide templates in word/excel form in which physical data for the migration purpose may be inserted by PFRDA.
2. It is SI's responsibility to work with respective data owners in PFRDA to verify and obtain approvals for all the data transformed and further ensure its quality, accuracy, integrity, confidentiality and completeness.
3. SI is expected to migrate data before go-live of the project.
4. Develop a rollback plan and contingency measures in case any issues or errors arise during the data migration process, ensuring a fall back option to the legacy system if needed.

i) Security Audit and Vulnerability Assessment and Penetration Testing (VAPT):

Prior to the Go-Live phase of this project, the selected Service Integrator (SI) shall engage a third-party agency that is empanelled with [CERT-IN] (hereinafter referred to as the 'Empanelled Agency') to conduct a comprehensive Security Audit and Vulnerability Assessment and Penetration Testing (VAPT) on all aspects of the system. All cost of the security audit & VAPT to be borne by SI. SI shall obtain a certificate from the Empanelled Agency confirming compliance with the required security standards.

Furthermore, SI shall commit to conduct Security Audit and VAPT annually as compliance. Additionally, in the event of a security breach, SI shall, at its own cost, engage the Empanelled Agency to re-evaluate and rectify any security vulnerabilities discovered during the breach assessment. SI shall re-obtain a certificate from the Empanelled Agency confirming compliance with the required security standards once the event has been rectified & proofed. All confidentiality obligations applicable to SI shall be made applicable by SI to such an agency.

j) Licensing

1. SI would be required to provide Enterprise-wide all-inclusive based licences considering all functionalities, features, and modules as per the requirements of PFRDA for entire project duration for the entire proposed solution with extensions or renewals post completion of contract. SI must ensure that the entire solution is hosted on a GCC or VPC which is empanelled with MeitY.
2. The total number of proposed solution users is expected to be around Seven Hundred and Fifty (750) users with One hundred (100) concurrent users and annual growth of 10% - 20% in both. However, the number of users is subject to change thus it is expected that OEM's –Solution must offer licences considering the no. of users given and estimated growth rate and incorporate in their financial bid. PFRDA will not bear any additional expenses for any type of license during project duration. The right to use the software will be across all intermediaries who may login from anywhere in the country.
3. All licenses to be procured by the SI shall be in the name of PFRDA and shall be perpetual in nature for the TRACE project and should be usable on any cloud /software/database platforms whether on premises or on cloud environments. In case some software licenses which are required to be used by the bidder in the project are subscription based, such subscription cost to be borne by the SI and PFRDA would not pay any extra amount for the same during the entire project tenure. Therefore, all such costs if any shall be included in the Financial Bid submitted by the bidders. SI shall not withhold or fail to procure such licenses, in any manner, as are required for successful implementation of the project.
4. No extra licence fees/implementation charges should be charged by SI for implementing the software in the test environment and at the Disaster Recovery site.

5. Any cost which is further required for the purpose of solution version upgrade, updates, patches, technology refreshes should be part of the licensing/subscription cost of the proposed solution for the entire project duration. Bidders to take the same into consideration while including total cost for the same in the financial bid.
6. SI should ensure that while applying software patches and in the version migration, the developed/customised software is also properly migrated to such higher versions or extended versions. It is SI's responsibility to ensure that any customization is compatible with upgraded applications/modules at no extra cost to PFRDA.
7. SI shall ensure that newer versions are backward compatible with all the devices which run on any version of the operating systems for which the respective companies are still providing support.
8. If at all an OEM product/solution becomes obsolete or non-operational and further discontinues its solution for whatsoever reason during the entire project tenure, SI & OEM will have to honour the contract to continue to provide all agreed services and support for the OEM product assuring 100% business continuity. SI shall be held to be in breach, if it fails to do so whereby the timely implementation of the project is hampered at any point of time.
9. User/ License/Subscription charges will be applicable for entire project duration, In case, if the project is extended, the System Integrator (SI) will bear the costs of licenses/subscription charges for the entire extended duration,

k) Implementation/Go live

Go-Live is the phase in which the software solution in terms of this RFP is made available to respective PFRDA official/stakeholders.

1. Before the final Go-Live, SI has to complete development, customization, configurations, and third-party integrations of the application as per the Functional, Non-Functional, Security and Technical Requirement Specifications as stated in RFP.
2. The Go-Live is an end-to-end responsibility of SI who will manage total planning, hand holding support as per the scope of work.
3. The completion shall include satisfactory completion of all the functional, non-functional, technical, security requirements, installation, data migration, testing, deployment etc.
4. In case of the Go-Live delays by SI, the compensation for delay will be payable/recoverable by PFRDA as per SLA and Liquidated damages defined in this RFP document. However, if the delays happen due to any approval/clearance pending from PFRDA side, the same may be documented and concurred by PFRDA and in such case no recovery will be applicable.
5. The implementation phase shall be deemed as completed in all respects only after:
6. All applications and services are implemented as per the intent of this RFP scope to the satisfaction of PFRDA.

7. Entire Solution and associated components meet all the necessary security test as part of Secure Software Development Lifecycle (SSDLC) methodology and Government Guidelines.
8. All requirements and scope mentioned in this RFP have been completed with signoffs.
9. SI shall be solely responsible for the procurement and installation of all the required suitable solutions including software licences in the name of PFRDA and sourcing of cloud services including sizing from CSP. All security requirements such as 3rd party software and security audit clearance certificate from CERT-IN empanelled vendor shall be the sole responsibility of SI. SI shall also be responsible for all security aspects including disaster Management activities such as complete backup of APIs, code, and data etc. for the integrated solution.

l) Stabilization cum Warranty phase

1. Responsibilities/SoW of SI during Stabilization Phase:
    a. **Duration:** It would be mandatory for SI to provide a Warranty & Stabilization phase for One (01) Year for the solution to be developed by it. The Stabilization period would commence from the date of implementation/go live date of the project and acceptance/sign-off on go-live from PFRDA.
    b. **Objective**: The stabilization phase would be focused on optimizing and stabilizing the system's performance.
    c. **Performance Tuning:** During the stabilization phase, the emphasis would be on fixing defects, performance tuning, optimization, and ensuring that the system meets the agreed-upon performance benchmarks.
    d. **Monitoring and Maintenance**: The SI will further detail out ongoing monitoring and maintenance activities to ensure the continued stability and efficiency of the system.
    e. **Scalability Planning**: SI in accordance with PFRDA may need to plan for scaling the infrastructure based on usage patterns and performance requirements.
    f. **Performance Optimization:** Analyse the software's performance and address any bottlenecks or performance-related issues. Optimise code, database queries, and system configurations to improve overall performance.
    g. **Compatibility Testing:** Ensure that the software is compatible with various operating systems, browsers, and devices. Address any compatibility issues that may arise.
    h. **Documentation:** Update and finalise project documentation, including user manuals, technical documentation, and release notes. Ensure that all documentation is accurate and comprehensive.
    i. **Monitoring and Logging:** Implement monitoring tools and logging mechanisms to track system performance and detect issues in real-time. Set up alerts and notifications for critical events.

j. **Training and Knowledge Transfer:** Provide training to PFRDA and/or end-users as needed to ensure that they can effectively support and maintain the software. Transfer knowledge about the software's architecture and maintenance requirements.

k. **Backup and Disaster Recovery:** Implement robust backup and disaster recovery plans to safeguard data and ensure business continuity. Test and validate these plans to ensure they work effectively.

l. **Change Management:** Manage any requested changes or enhancements to the software during the stabilisation phase. Assess the impact of changes on stability and ensure proper testing and documentation.

m. **Support (Warranty/AMC)** would be comprehensive in nature and must have back-to-back support from the OEM/Service Provider. Service Provider/OEM will warrant products/services against defects arising out of faulty design etc. during the specified support period.

n. **Final Acceptance**: Work towards obtaining PFRDA's final acceptance of the software. The stabilisation phase is critical to ensure that the software is dependable, performs well, and meets user expectations before it is fully deployed and used by the client's organisation. It requires meticulous testing, optimization, and collaboration with stakeholders to achieve a successful transition to the production environment.

m) Training

1. SI should provide in person trainings to PFRDA's officials for using and managing the proposed system, which will include end user, technical and system Administration training. The training venue will be PFRDA office.
2. SI shall also provide trainings to officials of various intermediaries for using the solutions for data and compliance reporting. Since the intermediaries are located at different locations, the training may be conducted online in co-ordination with PFRDA.
3. Training phase includes preparation and submission of user manuals, handbooks, video tutorials etc. besides hands on classroom training sessions for PFRDA users.
4. Training materials for exiting PFRDA LMS & other modes to be prepared by SI & needs to be approved by PFRDA for existing & new features of the application which is to be tagged on their respective dashboards & email notifications.
5. For trainings, the training platform & related costs are to be borne by SI.

n) Setup Technical Helpdesk & Facility management team

1. A Technical helpdesk to be setup by SI via Email, Telephone (with Interactive Voice Response (IVR) narrating wait time & cue number, Call detail record (CDR), feedback SMS, Communication SMS. The helpdesk should be operated via a CRM where ticketing is used for every event. Reports are created as per PFRDA need. Incident

Management/Ticketing tools will be provided by SI for handling issues, requests, concerns raised by PFRDA users during entire project duration.

2. In addition to the helpdesk, another two resources are required to be stationed at PFRDA premises as facility management team from 9.30 am to 6.00 pm, from Monday to Friday (all working days) for a period of One (01) Year time duration from start of the Stabilisation & Warranty phase, for the tasks given below:
    a. Assist PFRDA employees in case any support is needed for using the application.
    b. Work together with PFRDA employees to gather inputs for any issues in the application faced by the users and communicate the same to bidder's offshore team.
    c. Conduct solution demonstration as and when required.
    d. Requirement gathering or any future enhancements/changes or Continuous Development.

Any other work related to the proposed solution, if required during the Stabilization & Warranty or AMC period, if scope of work is diversified requiring a different skilled resource/workforce other than the two-manpower deployed, then SI shall have to improvise to deliver the requisite resource person to PFRDA at no additional cost.

o) AMC Support

It covers ongoing maintenance and support for the software beyond the initial warranty period. An AMC outlines the terms under which SI will provide updates, bug fixes, feature enhancements, and technical support to ensure the software's continued functioning and relevance. An AMC may cover a range of services, such as, but not limited to:

1. Bug Identification and Resolution: Employ monitoring tools and user feedback channels to identify and categorise software issues. Establish a systematic process for tracking, prioritising, and resolving reported defects. Collaborate with development teams to address complex or critical issues promptly. Ensure that fixes do not introduce new problems through comprehensive testing and regression testing.
2. Performance Monitoring and Optimization: Implement comprehensive performance monitoring solutions to proactively detect bottlenecks and performance issues. Conduct regular performance audits to identify areas for improvement. Optimize code, database queries, and configurations for optimal system performance. Plan capacity upgrades and scalability improvements as needed. Compatibility updates to ensure the software remains compatible with evolving technologies and platforms.
3. Feature enhancements or additions based on PFRDA requirements.
4. Technical support to assist users in case they encounter issues while using the software.
5. Performance optimization to keep the software running smoothly as the user base or data load increases.

6. Data Backup and Recovery Management: Establish automated backup routines for data and configurations. Periodically test data recovery procedures to ensure they work as expected. Maintain a comprehensive disaster recovery plan, including off-site backups and failover solutions. Be prepared to swiftly recover from data loss or system failures.
7. Documentation Management: Keep all documentation updated and organized. Document changes, fixes, and enhancements made during the maintenance phase. Ensure that user manuals and technical documentation are accurate and comprehensive. Offer self-help resources and knowledge base articles for common user queries.
8. Change Management and Request Handling: Establish a formalized change management process for handling enhancement requests and change proposals. Assess the impact of requested changes on system stability, security, and performance. Prioritize and schedule approved changes for implementation.
9. License and Compliance Oversight: Maintain records of software licenses and ensure compliance with licensing agreements. Schedule and oversee license renewals and updates. Keep track of compliance with industry regulations and standards.
10. Reporting and Analytics: Generate regular reports and dashboards summarizing system performance, support ticket trends, and SLA adherence. Use analytics to identify patterns, anomalies, and areas requiring attention. Share insights with stakeholders to inform decision-making and improvements.
11. Project Communication and Review Meetings: Maintain transparent and ongoing communication with PFRDA stakeholders. Hold regular review meetings to discuss the state of the system, performance, and planned maintenance activities. Address PFRDA concerns and expectations promptly.
12. Service Level Agreement (SLA) Adherence: Strictly adhere to SLAs defined in maintenance contracts, including but not limited to response times, resolution times, and availability commitments. Continuously measure and report on SLA compliance.
13. Proactive Maintenance and Preventive Measures: Develop proactive maintenance plans to identify and mitigate potential issues before they impact users. Conduct routine system health checks, security scans, and vulnerability assessments. Implement predictive analytics and monitoring to anticipate future needs and trends.
14. Cost Management and Budgeting: Maintain a detailed budget for maintenance activities, including software licences, support contracts, personnel, and infrastructure costs.
15. Continuous Improvement Initiatives: Encourage a culture of continuous improvement within the maintenance team. Solicit feedback from users and stakeholders to identify areas for enhancement. Implement process improvements and system optimizations based on lessons learned.
16. AMC should ensure ongoing maintenance, support, and updates beyond the initial warranty period, helping to ensure the software's continued functionality and relevance over time.
17. SI shall be responsible for recovery of lost data, restoration and repair of damaged data and the correction of data.

18. SI shall be responsible for a well-defined document for backup and restore policy on the available database. In case of upgradation of system software and database, SI shall provide a revised version of backup and restore policy document.
19. SI shall provide a well-defined document for extensive security features at the system and database levels to ensure security and integrity of the Data and the Application Modules
20. SI shall provide a well-defined document for auditing the system. It shall include an audit trail across all modules by associating user id, data, and time stamp with add, changes, and deletes during any change carried out in file structure, database, and applications.
21. The complete solution has to be secured by design, end to end encryption as per the latest standards, masking of data fields wherever required and also as advised by PFRDA, complied with all security measures that means all security provisions to be taken care of while designing application, product, database, or integrated framework.

p) Change Management

This Change Management scope outlines the responsibilities and procedures necessary to manage changes effectively during the entire project duration, ensuring that any modifications are executed with minimal disruption and maximum benefit to the project and its stakeholders.

Change Control Board (CCB): The Change Control Board consisting of officers of PFRDA, and representative of SI may be constituted by PFRDA and the same CCB or designated authority will be responsible for overseeing the change management process, ensuring compliance with policies and procedures, and making final decisions on change requests.

Change management covers the following:

1. Change Request Submission and Evaluation: During the project tenure, the Change Management process will be integral to the successful operation of the project. The scope includes:
    a. Receipt of change requests.
    b. Initial evaluation and categorization of change requests.
    c. Assessment of potential impacts on the project, including costs, timelines, and resource requirements.
2. Prioritization and Approval:
    a. Prioritization of change requests based on their impact, urgency, and strategic alignment.
    b. Approval or rejection of change requests by the designated Change Control Board or designated authorities.
3. Change Implementation: Once approved, the change will move into the implementation phase, which covers:

a. Detailed planning of the change implementation, including resources, schedule, and communication.
b. Development and testing of the change in a controlled environment.
c. Documentation of changes, including updated project documentation, test plans, and user guides.
d. User training, if necessary.
e. Implementation and deployment of the change into the production environment.

4. Testing and Quality Assurance:
    a. Comprehensive testing of the change, including functional, regression, and integration testing.
    b. Verification of quality and performance against pre-defined standards.
    c. Identification and resolution of issues or defects.
5. Communication and Stakeholder Engagement:
    a. Effective communication with relevant stakeholders about the approved changes.
    b. Providing advance notice, instructions, and necessary support to impacted users or teams.
6. Monitoring and Review:
    a. On-going monitoring and tracking of implemented changes.
    b. Periodic reviews to assess the effectiveness and impact of changes on project performance and user satisfaction.
    c. Adjustment of change management processes based on lessons learned.
7. Documentation and Reporting:
    a. Comprehensive documentation of all changes, including records of approvals, implementation details, testing results, and user feedback.
    b. Regular reporting to project stakeholders, and relevant teams on the status and outcomes of change requests.
8. Continuous Improvement: Throughout the project tenure, there will be an emphasis on continuous improvement:
    a. Analysing the change management process and identifying areas for enhancement.
    b. Implementing best practices and process improvements to increase efficiency and effectiveness.
9. Emergency Change Management: In cases of critical or emergency changes that require immediate attention, the scope includes expedited evaluation, approval, and implementation to minimize disruption and maintain operational integrity.
10. Compliance and Documentation: SI will ensure compliance with all relevant documentation, reporting and regulatory requirements related to change management.

11. Escalation and Issue Resolution: The scope also includes a defined process for resolving disputes, issues, or concerns related to change requests, prioritization, or implementation.
12. Resource Management: Allocation of necessary resources, including personnel, tools, and technology, to support the Change Management process.

SI shall allocate a credit of Five hundred Change Request man-days (500) as pre-included efforts for the entire tenure of the project, starting from the date of Go-Live. Bidders are required to incorporate this amount in their respective section of the bid.

In addition to the pre-included CR man-days (500-man days) (to be paid on actual as being used & billed), SI is required to quote man days rate for various resources that PFRDA may consider using for CR services during the project tenure in the prescribed format given at ***Annexure- XIV***. It may be noted that PFRDA will invoke these rates for any further Change Requests once the efforts under man month as quoted in Man month bundle have been exhausted.

The Change Control Board (CCB) will be responsible for overseeing the change management process, ensuring compliance with policies and procedures, and making final decisions on change requests.

1. All changes outside the scope of work or Schedule of Services having financial implications in terms of the overall cost/time of the project, shall be undertaken by SI, only after securing the written consent of PFRDA.
2. While approving any change request, if required, PFRDA may ask SI to deploy the required resources on-site.
3. The change request/management procedure will follow the following steps:
    a. The information related to initiator, initiation date and details of change required, and priority of the change will be documented by PFRDA.
    b. Impact of the change in terms of the estimated effort, changed schedule, cost and the items impacted will be analysed and documented by SI.
    c. CCB will approve or disapprove the change requested including the additional payments (as per the quoted man- month rate), after discussion with SI on the impact of the change on schedule.
    d. Any change request where the total man- month effort requirement is up to the ten (10) man-days shall not be considered as change request.
    e. The change will be implemented in accordance with the agreed cost, effort, and schedule.

The change will be verified and assessed by PFRDA on completion of implementation of change request prior to deployment on the production server.

q) Scalability & Capacity Planning

The solution should be scalable to cater PFRDA futuristic requirements in terms of Application and Infrastructure both. Please refer to the indicative Technical Specification document in ***Schedule III.***

10. Project Schedule and Milestones

The total period of the project will be **six (06) years** comprising of T**welve (12) months of development** and implementation period (Go-live) from the date of the award of the contract, followed by **Twelve (12) months of warranty & stabilisation and then Forty-eight (48) months for AMC.**

Milestones	**Indicative Key Deliverables/Activities**
Issue of Letter of Intent/Award	Work Order
Signing of Agreement/Contract	Within 30 days of receiving the Letter of intent (LoI)from PFRDA
Start-Off/Kick-off Meeting	- Project Charter
	- Project Plan
	- Kick-off Meeting Agenda
	- Stakeholder List
Requirement Gathering (As-Is & To-Be Analysis)	- Business Process Documentation
	- User Interviews
	- Requirement Elicitation Report
	- Use Case Diagrams
	- User Stories
Documentation: BRD, FRS, SRS, Design Guidelines, SDD, etc.	- Business Requirements Document (BRD)
	- Functional Requirements Specification (FRS)
	- System Requirements Specification (SRS)
	- Design Guidelines
	- System Design Document (SDD)
Infrastructure for Dev-Ops	- Infrastructure Design Document
	- Services and Software Inventory

Milestones	Indicative Key Deliverables/Activities
	- Network Configuration Documents
Development: Customization, Configuration, 3rd party Integration	- Code Repository
	- Customization Specifications
	- Integration Documentation
	- Configuration Settings, Source Code, Customization build, APIs
UAT Deployment	- Deployment Plan
	- Rollout Schedule
	- Deployment Checklist
UAT Testing	- Test Plan
	- Test Cases
	- Test Scripts
	- Test Reports
Licensing	- Software Licensing Agreements
	- License Inventory
Security Audit and Vulnerability Assessment and Penetration Testing (VAPT)	- Security Audit Report - VAPT Report - Remediation Plan
Implementation/Go Live	- Go Live Plan - Rollback Plan
Setup Helpdesk	- Helpdesk Documentation
	- Support Ticketing System
Training	- Training Plan
	- Training Materials
	- Training Attendance Records
Warranty cum Stabilization phase	- Warranty Agreement
	- Warranty Period Documentation
	- Stabilization Plan

Milestones	Indicative Key Deliverables/Activities
	- Stabilization Reports
AMC Support	- Annual Maintenance Contract (AMC) Agreement
	- AMC Support Plan
Change Management	- Change Request Forms
	- Change Management Process Documentation

As the project envisages various modules and different requirements from different stakeholders/intermediaries, SI shall plan various stages as per progress under that particular module without inter-dependence on progress of other modules. Agile methodology should be followed.

In case of delay in completion of milestone(s) due to any reason(other than on account of any delay attributable to PFRDA) which is likely to result in enhancement of time duration for submission of the respective deliverables, in such an event, the tenure of the contract may be extended, at the instance of PFRDA. The SI shall be required to fulfil its obligations, without any additional cost to PFRDA.

11. Payment terms

1. Payment will be made on successful completion of Milestone to the satisfaction of PFRDA as defined at ***Annexure-IX,*** upon submission of Invoice from SI and approval of PFRDA on the same.
2. Any delay in achievement of milestones/deliverables/activities from SI shall automatically result in delay of corresponding payment from PFRDA without any additional liability on PFRDA.
3. Any objection/dispute/clarification to the amounts invoiced in the bill will be raised by PFRDA within reasonable time from the date of receipt of the invoice. Upon settlement of disputes with respect to any disputed invoice(s), PFRDA will make payment within thirty (30) working days of the settlement of such disputes.
4. Terms of payment indicated in the Contract that will be signed between PFRDA and SI will be final and binding on SI and no interest will be payable by PFRDA on outstanding amounts under any circumstances, if there are any clauses in the Invoice contrary to the terms of the Contract.

12. Taxes and duties

1. Prices quoted should be exclusive of GST but inclusive of all other taxes/duties/levies as also cost of incidental services such as transportation, road permits, insurance etc.

Bidders shall include all such taxes in the contract price. PFRDA shall not be liable to pay any other taxes/levies/duties except for GST for invoices in the name of PFRDA. The total price quoted by bidder exclusive of GST as applicable will be considered for financial bid evaluation. Any new levies or taxes after award of contract shall be borne by party to whom contract has been awarded.

2. All expenses, stamp duty and other charges/expenses in connection with the execution of the Agreement arising out of this RFP process shall be borne by the SI.
3. Wherever the laws and regulations require deduction of such taxes at the source of payment, PFRDA shall make such deductions from the payment due to the SI. The remittance of amounts so deducted and issuance of certificate for such deductions shall be made by PFRDA as per the laws and regulations for the time being in force. Nothing in the Contract shall relieve SI from his responsibility to pay any tax that may be levied on income and profits made by SI in respect of this Contract.

13. Eligibility Criteria

1. Bid is open to all interested Bidders who meet the eligibility criteria as given in ***Annexure-V***. The eligibility conditions have to be satisfied on the date of submission of respective bids.
2. During evaluation and comparison of Bids, PFRDA may, at its discretion, ask bidders for clarification on the Bids received. The request for clarification shall be in writing and no change in Financials or substance of the Bid shall be sought, offered, or permitted. No clarification at the initiative of bidder shall be entertained after the bid submission date. No conditional bid shall be accepted from any bidder.

14. Technical Evaluation Criteria

1. Bids will be evaluated by the Quality cum Cost Based Selection (QCBS) method.
2. Eligible bidders to be technically evaluated as per the Technical Evaluation criteria given at ***Annexure-VI*** of this document. Bidder must submit the documents substantiating eligibility and Technical Evaluation criteria as mentioned in this RFP document.
3. Technical evaluation will include technical information, demonstration of proposed Technology Solution/services, reference calls and site visits, wherever required. Bidders may highlight the noteworthy/superior features of their Technology Solution/services. Bidder to demonstrate/substantiate all claims made in the technical Bid along with supporting documents to PFRDA.
4. Bidders who qualify the eligibility criteria, will be called for an in-person presentation of the solution that must include Solution Approach (led by the Key Personnel mentioned in the technical bid document), Solution architecture, proposed benefit of the recommended technology stack, implementation methodology, project management approach, cloud deployment methodologies, etc. This should include both Functional and Non-Functional approaches.

15. Financial Evaluation Criteria

1. Bidders to submit financial bid in the prescribed format as given at ***Annexure- VIII***.
2. Bidders who score 70 or more out of 100 marks in the technical evaluation will be declared as Technically qualified. Financial bids of only technically qualified bidders will be opened.

An illustration for the process of Combined Technical–Financial Evaluation process is given below:

a) Combined Technical–Financial Evaluation process.

In respect of all the technically qualified bidders, in whose case, the financial bid has been opened; a combined techno-financial evaluation will be done by PFRDA as per the following procedure:

1. Technical score will be arrived at treating the marks of bidder scoring the highest marks (A) in Technical evaluation as 100. Technical score for other bidders (B, C etc.) will be computed using the formula, T= Marks of B/Marks of highest scorer A * 100.
2. Similarly, financial score of all technically qualified bidders will be arrived at taking the cost quoted by L1 bidder i.e., the lowest quote from all technically qualified bidders (say F) as 100. Marks for other bidders will be calculated using the formula Combined Score = Cost of L1 bidder (F)/Cost quoted by bidder * 100.
3. A "Combined Score" will be arrived at, considering both marks scored through technical bid evaluation and the financial quotes with a weight age of 70% for technical and 30% for financials as detailed below.
4. Then combined score is arrived at by adding Technical Score and Financial Score. The successful bidder will be the one who has the highest Combined Score (H1), up to 2 decimals.
5. Formula for calculating the Combined Score of technically qualified bidder is as follows.
6. H = (T/T High x 70) + (F Low/F x 30)
7. Whereas: H = Combined Score
8. T=Technical Score; T High = Highest Technical Score among bidders
9. F=Financial Quote; F Low = Lowest financial quote of F among bidders

Example:

Bidder	Technical Evaluation Marks (T)	Nominal Bid Price in INR (F)	Technical Score	Commercial Score	Combined Score (out of 100)
A	95	71	95/95*70=70.00	60/71*30=25.35	70.0+25.35=95.35 (H-1)
B	85	65	85/95*70=62.63	60/65*30=27.69	62.63+27.69=90.32 (H-2)
F	80	60	80/95*70=58.94	60/60*30=30.00	58.94+30=88.94(H-3)

In the above example, Bidder A with highest score (H1) becomes the successful Bidder. In case of a tie between bidders i.e., if two or more bidders receive the same combined score, bidder with the higher technical score shall be declared as (H1).

16. Award of contract

Award of contract to the Bid scoring highest marks based on QCBS method (Quality and Cost Based Selection) combining score of bids giving weightage of **Seventy – Thirty** (70:30) for technical and financial scores, respectively.

1. Up to two decimal points (rounding off) will be taken in the final score. If two or more bidders receive the same combined score, bidder with the higher technical score shall be declared as (H1).
2. Bidder with highest score (H1) becomes the successful Bidder. In case of a tie between bidders i.e., if two or more bidders receive the same combined score, bidder with the higher technical score shall be declared as (H1).
3. PFRDA will notify 'Selected Bidder/Awardee/SI' in writing by way of issuance of Letter of Intent (LOI) that its Bid has been accepted. SI must return the duplicate copy of the same to PFRDA within Ten (10) working days, duly Accepted, Stamped and Signed by Authorised Signatory of the SI as a token of acceptance.
4. The successful Bidder will have to execute a Non-Disclosure Agreement (NDA) as per ***Appendix-V***, Performance Security/Performance Security for the amount and validity as desired in this RFP on the lines of indicative format given in ***Appendix-II*** of this RFP before signing of the Master Service Agreement. The NDA shall be valid even post contract completion up to 180 days.
5. The successful Bidder shall be required to enter into a Contract with PFRDA. Copy of Board resolution and power of attorney (POA wherever applicable) showing that Signatory has been duly authorized to sign the acceptance letter, contract and NDA should be submitted to PFRDA.

6. PFRDA reserves the right to stipulate, at the time of finalization of the Contract, any other document(s) to be enclosed as a part of the final Contract.
7. Failure of the successful Bidder to comply with the requirements/terms and conditions of this RFP shall constitute sufficient grounds for the annulment of the award and forfeiture of the EMD and/or Performance Security.

17. Clarification and Amendments on RFP/Pre-bid meeting

1. Any Bidder requiring clarification on RFP may notify PFRDA in writing strictly as per the format given in ***Annexure-IV*** at the email address within the date/time mentioned in the Schedule of Events.
2. A pre-Bid meeting will be held in person or online or in both mode on the date and time specified in the *Schedule of Events* which may be attended by the authorized representatives of bidders interested to respond to this RFP.
3. The queries received (without identifying source of query) and response of PFRDA thereof will be posted on PFRDA's website or conveyed to bidders.
4. PFRDA reserves the right to amend, rescind or reissue the RFP, at any time prior to the deadline for submission of Bids. PFRDA, for any reason, whether, on its own initiative or in response to a clarification requested by a prospective Bidder, may modify the RFP, by amendment which will be made available to bidders by way of corrigendum/addendum. The interested parties/bidders are advised to check PFRDA's website regularly till the date of submission of Bid document specified in the *Schedule of Events*/*email* and ensure that clarifications/amendments issued by PFRDA, if any, have been taken into consideration before submitting the Bid. Such amendments/clarifications, if any, issued by PFRDA will be binding on the participating Bidders. PFRDA will not take any responsibility for any such omissions by bidder. PFRDA, at its own discretion, may extend the deadline for submission of Bids in order to allow prospective Bidders a reasonable time to prepare the Bid, for taking the amendment into account.
5. No request for change in Financial/legal terms and conditions, other than what has been mentioned in this RFP or any addenda/corrigenda or clarifications issued in connection thereto, will be entertained and queries in this regard, therefore will not be entertained.
6. Queries received after the scheduled date and time will not be responded/acted upon.

18. Contents of Bid document

The Bid prepared by bidder, as well as all correspondences and documents relating to the Bid exchanged by bidder and supporting documents and printed literature shall be submitted in English.

The information provided by bidders in response to this RFP will become the property of PFRDA and will not be returned. Incomplete information in the Bid document may lead to non-consideration of the proposal.

19. Powers to vary or omit work

In any case in which the successful Bidder has received instructions from PFRDA as to the requirements for carrying out the altered or additional substituted work which either then or later, will in the opinion of the SI, involve a claim for additional payments, such additional payments shall be in line with Change request rates and mutually agreed with the terms and conditions of the order.

20. Bid processing fee

1. Bidders to submit Bid Processing Fee (INR 25,000 i.e., Rupees Twenty-Five Thousand Only) plus GST @ 18% i.e. Rs. 4,500/- (Total of Rs. 29,500). Bidders shall transfer the aforementioned amount through electronic transfer in the designated bank account of PFRDA or in the form of Account payee demand draft in favour of PFRDA, New Delhi. Details of bank account is given in table of ***Schedule of events.***
2. Bidders who have submitted bid proposals against EOI for TARCH project Ref no.: PFRDA/2022-23/IT/02 issued on 27 June 2022 and not submitted bid for RFP ref. no. : PFRDA/2023/TARCH/PINTRA/01 issued on 4th July 2023 are exempted from submitting Bid processing fee.

21. Earnest Money deposit (EMD)

1. Bidder shall furnish EMD for the amount and validity period mentioned in the Schedule of Events of this RFP.
2. EMD should be submitted by the bidders in the form of a Performance Bank Guarantee (BG)/Fixed Deposit Receipt - issued by a Scheduled Commercial bank lien marked in favour of PFRDA /Online Payment in the designated bank account of PFRDA. The EMD submitted in the form of bank guarantee/Fixed deposit receipt should be valid up to at least 180 days from the bid submission end date.
    a. Any Bid not accompanied by EMD for the specified amount and not submitted to PFRDA as mentioned in this RFP will be rejected as non- responsive.
    b. The EMD of the unsuccessful Bidder will be discharged and returned within one month upon notification of award to the successful Bidder.
    c. The EMD of the successful Bidder will be discharged upon bidder signing the Contract and furnishing the Performance Security for the amount and validity as mentioned in this RFP.

    Note :- The EMD format outlined as ***Appendix - I*** shall be considered as indicative, and PFRDA reserves the right to accept EMD presented in accordance with the format, without prejudice to the accuracy and completeness of the information contained therein.

    a. The EMD may be forfeited:

b. if a Bidder withdraws or modify the submitted Bid during the period of Bid validity specified in this RFP; or

c. if a Bidder makes any statement or encloses any form which turns out to be false/incorrect at any time prior to signing of Contract; or

d. if the successful Bidder fails to accept Letter of Intent and/or sign the Contract with PFRDA or furnish Performance Security, within the specified period in the RFP.

e. If EMD is forfeited for any reasons mentioned above, the concerned Bidder may be debarred from participating in the RFPs floated by PFRDA, in future, as per sole discretion of PFRDA.

3. No interest would be paid by PFRDA on EMD or Performance Security received in the account of PFRDA, under any circumstances.
4. Micro and Small Enterprises (MSEs) as defined in MSE Procurement Policy issued by Department of Micro, Small and Medium Enterprises (MSMEs) or are registered with the Central Purchase Organization or the concerned Ministry or Department or Start-ups as recognized by Department of Industrial Policy & Promotion (DIPP) are exempted from submission of EMD.

22. Bid Preparation and Submission

I. Bid Preparation

The Bid prepared by the bidders shall comprise the following components:

1. Technical Bid – Technical Bid shall comprise of:
   a. EMD and Bid Processing fee in Original/Receipt
   b. Integrity Pact signed and stamped by Authorized Signatory
   c. Technical bid: Include copies of required documents along with required information as outlined in Eligibility and Technical Evaluation Parameters in this RFP and fulfils all the technical conditions of this document.
   d. Exit plan including Cloud port out plan
2. Financial Bid – Financial Bid as per the prescribed format as per ***Annexure-VIII***

   Each page of all the documents submitted by bidder shall be signed by authorized signatory and shall also put company's/authorized signatory' seal. Bidder's authorization shall be supported by attaching a scanned copy of valid proof of authorization like Power of Attorney/Board Resolution etc. binding the bidding entity.

II. Bid Submission

1. Bids must be properly secured and sealed. Bidders shall submit the complete Technical Bid. In addition, bidders shall also sign and stamp each page of Technical and Financial bid, as confirmation of their acceptance to the terms and conditions contained therein.

Further, bidders shall also sign with date and affix their seal of this RFP document and submit the same as part of technical bid.

2. Technical bid to be submitted in a separate envelope clearly marked "Technical Bid" with all relevant documents. Checklist for the documents to be submitted is provided at ***Annexure-XII***.
3. Care should be taken that the Technical Bid shall not contain any Financial information. Such proposal, if received, will be rejected.
4. Financial Bid shall contain the pricing terms strictly in the prescribed format as per ***Annexure-VIII*** to be submitted in a separate sealed envelope clearly marked "Financial Bid". The Price must include all the price components mentioned. Prices are to be quoted in Indian Rupees only.
5. The Total Financial bid shall include all licenses, subscriptions, services, software, database etc. without any exceptions for the entire duration of the contract. PFRDA shall not be responsible for any extra expenditure or any out of pocket expenses in this regard, whatsoever.
6. Bids must consist of the following envelopes:
    a. ***Envelope I*** will super scribing on top of the cover as "Envelope I: Bid Processing fee and Earnest Money Deposit and will be comprising of:
        i. **Bid processing fee** in the form of Account Payee Demand Draft. In case of online payment, receipt of the bid processing fee.
        ii. **Earnest Money Deposit (EMD)** in the form of Performance Security.
    b. ***Envelope II*** will super scribing on top of the cover as ***"Envelope II: Integrity Pact in Original"*** and will be comprising of:
        i. Integrity Pact in original
        ii. Integrity Pact is to be signed and submitted.
    c. ***Envelope III*** will super scribing on top of the cover as " Technical Bid" and will be comprising of:
        i. Technical bid along with all requisite documents as part of Technical bid including a softcopy in pen drive.
        ii. Exit plan including Cloud Port out plan
    d. ***Envelope IV***: will super scribing on top of the cover as "Financial Bid, in a sealed cover comprising of:
        i. Financial Bid

All the above four envelopes must be enclosed in a main envelope and marked with the caption '***DO NOT OPEN-THIS ENVELOPE TO BE OPENED BY PFRDA ONLY***' at the top with bid number and title to be submitted in the tender box provided for the purpose at the office of PFRDA addressed to,

Sh. Akhilesh Kumar,
Chief General Manager,
In charge- PFRDA-TRACE
Pension Fund Regulatory And Development Authority (PFRDA)
B-14/A, Qutab Institutional Area, Chhatrapati Shivaji Bhavan, Katwaria Sarai, New Delhi-110016

(Note: PFRDA is in the process of shifting its office at a different location in Delhi. In case the shifting happens before the bid submission end date, the same shall be notified on the PFRDA website (URL: www.pfrda.org.in). In such case, bidder is expected to submit its bid to the new address.)

RFP Reference No: PFRDA/2024/TARCH/PFRDA-TRACE/01

Bid Title: "REQUEST FOR PROPOSAL FOR SELECTION OF SYSTEM INTEGRATOR(SI) FOR DESIGN, DEVELOPMENT, IMPLEMENTATION AND MAINTENANCE OF PFRDA-TRACE (PFRDA - TRACKING REPORTING ANALYTICS & COMPLIANCE e-PLATFORM)

1. All inner and outer envelopes shall also indicate the name and address of bidder to enable the Bid to be returned unopened in case it is declared "late" i.e. received after due date and time. Once the Bid submission date and time is over, bidders cannot submit their Bid. Such bids will be declared 'late' bids and will be summarily rejected.
2. If the outer envelope is not sealed or marked, PFRDA will assume no responsibility for the same and such Bids will be summarily rejected.
3. The Bid document shall be complete in accordance with various clauses of the RFP document, or any addenda/corrigenda or clarifications issued in connection thereto, duly signed by the authorized representative of bidder. Document for authorizing representative to Bid and is to be attached.
4. Bid not accompanying the specified Bid processing fee shall be summarily rejected except for bidders who have submitted bid proposals against EOI for TARCH project Ref no.: PFRDA/2022-23/IT/02 issued on 27 June 2022 and have thereafter not submitted their bid for RFP ref. no.: PFRDA/2023/TARCH/PINTRA/01 issued on 4th July 2023.
5. If EMD is not submitted in accordance with the specified mentioned amount or is not in order otherwise, the submitted bid shall be summarily rejected except for Micro and Small Enterprises (MSEs) as defined in MSE Procurement Policy issued by Department of Micro, Small and Medium Enterprises (MSMEs) or are registered with the Central Purchase Organization or the concerned Ministry or Department or Start-ups as recognized by Department of Industrial Policy & Promotion (DIPP).
6. If a bidder quotes NIL charges/consideration or quotes unrealistically low bid, the bid shall be treated as unresponsive and will not be considered.

7. If deemed necessary, PFRDA may seek clarifications on any aspect from bidder. However, that would not entitle bidder to change or cause any change in the substances of the Bid already submitted or the Financial quoted.
8. Bidders may also be asked to give presentation for the purpose of clarification of the Bid.
9. Bid received without signed Integrity pact will be summarily rejected.
10. Bidder must provide specific and factual replies to the points raised in the RFP.
11. The Bid shall be typed or written and shall be signed on each page by bidder or a person or persons duly authorized to bind bidder to the Contract.
12. All the enclosures (Bid submission) shall be serially numbered.
13. Bidder(s) should prepare and submit their Bids well in advance before the prescribed date and time to avoid any delay or problem during the bid submission process. PFRDA shall not be held responsible for any sort of delay, or the difficulties faced by bidder(s) during the submission of Bids.
14. PFRDA reserves the right to reject Bids not conforming to above.
15. PFRDA reserves the right to accept or reject any Bid in part or in full or to cancel the bidding process and reject all Bids at any time prior to contract award as specified in Award Criteria and Award of Contract, without incurring any liability to the affected Bidder or Bidders or any obligation to inform the affected Bidder.

23. Modification and withdrawal of Bids

1. Bidder may modify or withdraw its Bid after the Bid's submission, provided modification, including substitution or withdrawal of the Bids, is received prior to the deadline prescribed for submission of Bids. In case the bidder opts for withdrawal or any modification or substitution in the bid, the bidder shall intimate its intent in writing with the revised documents and submit the same with properly mentioning the "Revision/Substitution" or Withdrawal and submit the same within the time of submission of bid. The bidder will be allowed to withdraw/revise/substitute the document as intended and submitted within the timelines of original submission , as the case may be at the time of opening of bid.
2. No modification in the Bid shall be allowed, after the deadline for submission of Bids.
3. No Bid shall be withdrawn in the interval between the deadline for submission of Bids and the expiration of the period of Bid validity specified in this RFP. Withdrawal or modification of a Bid during this interval may result in the forfeiture of EMD submitted by bidder.

24. Period of Bid Validity

1. Bid shall remain valid for the duration of 180 days from Bid submission date.
2. In exceptional circumstances, PFRDA may solicit bidders' consent to an extension of the period of validity. The request and the responses thereto shall be made in writing.

A Bidder is free to refuse the request. However, in such a case, PFRDA will not forfeit its EMD. However, any extension of validity of Bids or Financial will not entitle bidder to revise/modify the Bid document.

25. Bid Integrity

Wilful misrepresentation of any fact within the Bid will lead to the cancellation of the contract without prejudice to other actions that PFRDA may take. All the submissions, including any enclosed documents, will become property of PFRDA. Bidders shall be deemed to be licenced, and grant all rights to PFRDA, to reproduce the whole or any portion of their Bid document for the purpose of evaluation and to disclose the contents of submission for regulatory and legal requirements or such other purposes.

26. Bidding process/opening of technical bids

1. All the technical Bids duly received up to the specified time and date will be opened for initial evaluation on the time and date mentioned in the schedule of events. The envelopes containing the Bid Processing Fee, EMD and Integrity Pact will be opened in the presence of representatives of bidders who choose to attend the same. At the time of opening of these envelopes, it will also be ascertained whether the technical bid and financial bids have been submitted separately in the sealed envelopes. The representatives present will be required to sign the attendance sheet and also on the sealed financial bids conforming receipt of the same in sealed status from all bidders. Bids shall be opened at the scheduled time even if the representatives of all or any of bidders are not present.
2. In the first stage, only technical Bid will be opened and evaluated for eligibility criteria. Bids of such Bidders satisfying eligibility criteria and agree to comply with all the terms and conditions specified in the RFP will be evaluated for technical criteria.
3. Bidders scoring minimum 70 out of total 100 marks in technical evaluation shall be eligible for opening of financial bids.
4. PFRDA will form a bid opening cum evaluation committee to evaluate the bids and this committee will examine the Bids to determine whether they are complete, required formats have been furnished, the documents have been properly signed, processing fee, EMD for the desired amount and validity period is available and the Bids are in order. The committee may recommend to PFRDA and PFRDA may at its discretion waive any minor non-conformity or irregularity in a Bid which does not constitute a material deviation.

27. Contacting PFRDA

1. Any effort by a Bidder to influence members of the bid evaluation committee, PFRDA or its officials in its decisions on Bid evaluation and award of contract may result in the rejection of its Bid.

28. Consortium

As per scope of this RFP, consortium is not permitted. For clarification, consortium does not include collaboration with CSP & OEM for this project.

29. Subcontracting

As per scope of this RFP, subcontracting is strictly not permitted.

30. Services

1. All professional services necessary to successfully implement the proposed Software Solution will be part of the RFP/Contract.
2. SI should ensure that key personnel with relevant skill sets are available to always perform the contracted services.
3. SI should ensure that methodologies for delivering the services adhere to quality standards/timelines stipulated therefor.
4. SI shall provide and implement patches/upgrades/updates for software/Operating System/Middleware etc. as and when released by Service Provider/OEM or as per requirements of PFRDA. Whenever a new version update becomes available for a Major/Minor technology component (Example - database, development framework, CMS, etc), it is imperative for SI to notify the same to PFRDA within 2 weeks from the date of the release. This communication should be submitted with a recommendation proposal for version upgrade or otherwise. The proposal should be supported with an impact analysis report. The Change Control Board of the project will make the decision whether to retain the latest version, denoted as 'N,' or the immediately preceding version, 'N-1', for production & other environments of the project. In no scenario the versions should be beyond 'N-1'. No software proposed for use shall be in an alpha or beta version or remain unreleased as of the bid proposal submission date. The same should be applicable from the date of going live in production.
5. SI shall provide legally valid Software Solution and keep PFRDA safe and harmless against any claim under IPR. The detailed information on license count and type of license shall also be provided to PFRDA.
6. SI shall keep PFRDA explicitly informed of the end of support dates on related products/services/firmware and should ensure support during warranty and AMC.

31. SLA and compensation/Liquidated damage

The compensation will be applicable as mentioned in SLA and Liquidated damage- ***Appendix-IV*** of this RFP.

32. Right to Verification

1. PFRDA reserves the right to verify any or all the statements made by the bidders in the Bid document and to inspect bidder's facility, if necessary, to establish to its satisfaction about bidder's capacity/capabilities to perform the job.
2. The bidders are required to submit client references according to the specifications outlined in ***Annexure-X***.
3. PFRDA may visit/enquire and check the status from the mentioned clients.

33. Right to Audit

1. SI shall be subject to audit by internal/external Auditors appointed by PFRDA with respect to the project. SI shall facilitate the same. PFRDA can make its expert assessment on the efficiency and effectiveness of the security, control, risk management, governance system and process created by SI. SI shall, whenever required by the Auditors, furnish all relevant information, records/data to them. Costs for such audit will be borne by PFRDA. PFRDA will provide reasonable notice not less than seven (07) days to SI before such audit and same shall be conducted during normal business hours.
2. Where any deficiency has been observed during audit of SI on the risk parameters or in the certification submitted by the Auditors, SI shall correct/resolve the same at the earliest and shall provide all necessary documents related to resolution thereof and the auditor shall further certify in respect of resolution of the deficiencies. The resolution provided by SI shall require to be certified by the Auditors covering the respective risk parameters against which such deficiencies have been observed.
3. SI further agrees that whenever required by PFRDA, it will furnish all relevant information, records/data to such auditors and/or inspecting officials. PFRDA reserves the right to call for and/or retain any relevant information/audit reports on financial and security review with their findings undertaken by SI. However, SI shall not be obligated to provide records/data not related to Services under the Agreement (e.g., internal cost breakup etc.).

34. Validity of Agreement/Contract

The Agreement/SLA will be valid for the complete project duration as per the bifurcation given in Project Schedule.

35. Confidentiality

Service Provider shall treat all data and information of PFRDA as confidential, obtained in the process of executing its responsibilities, in strict confidence and will not reveal such information to any other party without prior written approval of PFRDA as explained under 'Non-Disclosure Agreement' in ***Appendix-VI*** of this RFP.

36. Delay in SI's performance

1. Delivery, installation, commissioning of the Software Solution and performance of Services shall be made by SI within the timelines prescribed.
2. If at any time during performance of the Contract, SI encounter conditions impeding timely delivery of the Software Solution and performance of Services, SI shall promptly notify PFRDA in writing of the fact of the delay, its duration, and cause(s). As soon as practicable after receipt of SI's notice, PFRDA will evaluate situation and may, at its discretion, extend SIs' time for performance, without their being any obligation to do so, in which case, the extension shall be ratified by the parties by amendment of the Contract.
3. Any delay in performing the obligation/defect in performance by SI may result in imposition of liquidated damages, compensation, invocation of Performance Security and/or termination of Contract (as laid down elsewhere in this RFP document) and as mentioned in the draft master service agreement.

37. Conflict of Interest

1. No Intermediary of PFRDA is allowed to participate in the bid process.
2. All bidders are required to disclose any actual or potential conflict of interest that may exist or arise during the course of the RFP process or any resulting contract. A conflict of interest arises when a bidder, its employees, or any of its associated entities have such a financial, personal, or other interest that could affect their impartiality or create an unfair advantage in this procurement process.
3. Bidders must promptly notify PFRDA of any such conflicts of interest. Failure to disclose conflicts of interest may result in disqualification from this RFP process or, if discovered after contract award, may lead to contract termination at the sole discretion of PFRDA.
4. PFRDA reserves the right to evaluate and address any conflicts of interest on a case-by-case basis and may request additional information or mitigation measures to ensure fairness, integrity, and transparency throughout the procurement process and the resulting contract.

38. Code of Integrity and Debarment

1. Bidders shall observe the highest standard of ethics/integrity during the bidding Process and in execution of the contract. Notwithstanding anything to the contrary contained herein, PFRDA shall reject Bid without being liable in any manner whatsoever to bidder if it determines that bidder was not eligible or has, directly or indirectly or through an agent, engaged in corrupt/fraudulent/coercive/undesirable or restrictive practices in the bidding Process.

2. Bidders are obliged under code of integrity to Suo-moto proactively declare any conflicts of interest (pre-existing or as and as soon as these arise at any stage) in RFP process and sign the Integrity pact as per Appendix III.
3. Participation of Bidders and their eligibility to participate in PFRDA's procurement is subject to compliance with code of integrity and performance in contract as per terms and conditions of the contract. Debarment from participation in PFRDA's procurement process in future shall be considered against bidders:
    a. if a Bidder is found to have directly or indirectly or through an agent, engaged or indulged in any corrupt/fraudulent/coercive/undesirable or restrictive practices during the bidding Process.
    b. Bidder fails to abide by the terms and conditions or to maintain the required technical/operational staff/equipment or there is change in its production/service line affecting its performance adversely or fails to cooperate.
    c. Other than in situations of force majeure, technically qualified bidder withdraws from the procurement process or after being declared as successful bidder: (i) withdraws from the process; (ii) fails to enter a Contract; or (iii) fails to provide performance guarantee or any other document or security required in terms of the RFP documents.
    d. If the Central Bureau of Investigation (CBI)/Central Vigilance Commission (CVC)/C&AG or Vigilance Department of PFRDA or any other investigating agency recommends such a course in respect of a case under investigation.
    e. If there is strong justification for believing that the partners/directors/ proprietor/agents of the firm/company have been guilty of violation of the code of integrity or Integrity Pact (wherever applicable), evasion or habitual default in payment of any tax levied by law; etc.
    f. Any other reason as deemed suitable by PFRDA.

39. Cloud Hosting requirements on Virtual Private Cloud/ Government Community Cloud

All the cloud related activities are the responsibility of SI as SI will be Single point of contact for PFRDA. The activities which are pertaining to CSP or MSP, SI will make sure that these activities will be performed as per standards like ITIL 4.0 framework. SI is expected to collaborate with Cloud Service Provider (CSP) and provide Virtual Private Cloud/Government Community Cloud to PFRDA for hosting PFRDA-TRACE for six (06) years comprising of Twelve (12) months of development and implementation period (Go-live) from the date of the award of the contract, Twelve (12) months of warranty & stabilisation and AMC for Forty-eight (48) months. As described in the Eligibility criteria, the Cloud Service Provider (CSP) should be MeitY empanelled and STQC audit compliant.

SI should host PFRDA-TRACE on MeitY empanelled cloud. SI, CSP & MSP need to make necessary provision for infrastructure, bandwidth scalability depending on the user load,

security & network arrangements. Apart from the **Production Environment, System Integrator shall maintain the Staging, UAT & Development environment**. SI shall justify the choice of development environment. SI shall list all tools to be used to develop, customize, and maintain the application, as well as the hosting platform, services and software & mention the same in ***Annexure XVIII***. SI shall be responsible for providing the Backup, Business Continuity Plan, Disaster recovery for the application and Disaster Recovery Operational Plan. SI shall ensure that the cloud services of only MeitY empanelled CSP is taken for the complete project duration.

SI shall ensure that Cloud Service Provider should also consider data growth while and hence scalability of the PFRDA-TRACE system in terms of compute, infrastructure Sizing (Hardware, network, bandwidth, firewall, webserver, application server, database server, IOPS, CPU, Memory, Storage) while submitting the bid.

SI shall ensure that CSP should implement Enterprise Management Software (EMS) Tools/management & monitoring services - required for various reports like Average Response Time during peak usage hours, application uptime, database performance etc. at no extra cost to PFRDA.

SI should prepare and submit a detailed plan during execution of order with following details, but not limited to:

Mapping of detailed services at primary site and DR site

1. VM Provisioning
2. Storage
3. Network interfaces
4. Network throughput
5. Backup

Detailed planning of services deployment and configuration:

1. Network architecture planning including
    a. VLAN configuration planning
    b. IP address planning
    c. Subnet planning and routing planning.
2. Firewall configuration planning
3. Backup methodology
4. Failover mechanism for replication links
5. SI should also submit ‘Cloud Port Out Plan’ along with the approach & methodology of the proposed project.

On acceptance of the Implementation Plan as submitted in the technical proposal SI shall implement the cloud solution. PFRDA may verify the related components/tools/approaches as

submitted in their technical proposal vis a vis implementation plan at any time of the project, if required.

40. Cloud Service Provider Requirements

The Cloud Service Provider shall comply or meet any security requirements applicable to Cloud Service Providers published (or to be published) by MeitY or any standards body setup/recognized by Government of India from time to time and notified to CSP/Service Providers by MeitY as a mandatory standard.

The Cloud Service Provider shall meet all the security requirements indicated in the IT Act 2000, the terms and conditions of the Empanelment of the Cloud Service Providers and shall comply to the audit criteria defined by STQC.

41. Managed Services Requirements

The below are managed services requirements for cloud management that should be performed for this RFP.

i. Backup Services

1. Should configure, schedule, and manage backups of all the data including but not limited to files, folders, images, system state, databases, and applications as per the policy developed by SI in consultation with PFRDA.
2. Shall be responsible for file system and database backup and restore services. As part of the responsibilities also to:
    a. Perform and store data and file backups (process of duplicating the users "to-be-backed- up" "Target Data") consisting of an initial full back up with daily incremental backups for files.
    b. For the files, perform weekly backups.
    c. For the databases, perform a twice weekly full database backup, with a three times daily backup of database log files.
    d. Cloud platform should provide Encryption of all backup files and data and management of encryption keys as a service that can be enabled for PFRDA that require such a service.
    e. Monitor and manage backup activity.
    f. Restore the requested data with the objective to initiate a minimum of 100 percent of the total number of restore requests per calendar month within a two-hour timeframe.
    g. Retain inactive versions of backed up flat files for 90 days and the last version of a deleted file for 180 days.
    h. Retain database backups for one hundred eighty (180) days.

i. All logs post the active storing tenure would be stored in archival storage.

j. Perform administration, tuning, optimization, planning, maintenance, and operations management for backup and restore.

k. Provide and install additional infrastructure capacity for backup and restore, as required, and perform backup on the next scheduled backup window in case of any scheduling conflicts between backup and patch management.

ii. Disaster Recovery & Business Continuity Services

1. In addition to the Primary DC, responsibility for Disaster Recovery Services so as to ensure continuity of operations in the event of failure of primary data centre and meet the RPO and RTO requirements. RPO should be less than or equal to 30 minutes and RTO shall be less than or equal to 120 minutes. PFRDA at its discretion in conjunction with the Implementing Agency may reduce the RPO and RTO during contract period. However, during the change from DC to DRC or vice-versa (regular planned changes), there should not be any data loss. There shall be asynchronous replication of data between Primary DC and DR DC. Responsibility includes sizing and providing the DC-DR replication link to meet the RTO and the RPO requirements.
2. The primary DC and the DRC should be from different physical locations supporting active – active/active-passive arrangement.
3. In case of any disaster, the security posture of the DR site shall be identical to the posture provided in the DC.
4. The disaster recovery site shall have Similar environment, processes, and controls (security, etc.) as that of the primary DC. During normal operations, the Primary Data Centre will serve the requests. During this period, the compute environment for the application in DR shall be available but with minimum possible compute resources required for a functional DR as per the solution offered. The application environment shall be installed and ready for use. DR Database Storage shall be replicated on an ongoing basis and shall be available in full (100% of the PDC) as per designed RTO/RPO and replication strategy. The storage should be 100% of the capacity of the Primary Data Centre site.
5. The scope of the DR drill lies with SI for planning & monitoring of the entire activity. In the event of a site failover or switchover, DR site will take over the active role, and all requests will be routed through that site. Application data and application states will be replicated between data centres so that when an outage occurs, failover to the surviving data centre can be accomplished within the specified RTO. This is the period during which the Compute environment for the application shall be equivalent to DC. The installed application instance and the database shall be usable, and the same SLAs as DC shall be provided. The Database and storage shall be of full capacity and the licenses and security shall be for full infrastructure. The bandwidth at the DR shall be scaled to the level of Data centre. Users of application should be routed seamlessly from DC site to DR site. SI along with CSP shall conduct DR drill for approximately two days at the interval of every six months of operation where in the Primary DC must be

deactivated and complete operations shall be carried out from the DR Site. However, during the change from DC to DRC or vice-versa (regular planned changes), there should not be any data loss.

6. Shall clearly define the procedure for announcing DR based on the proposed DR solution. Shall also clearly specify situations in which disaster shall be announced along with the implications of disaster and the time frame required for migrating to DR. Shall plan all the activities to be carried out during the Disaster Drill and issue a notice to the Department at least two weeks before such drill along with a risk mitigation plan & probable impact analysis report.
7. Should offer dashboard to monitor RPO and RTO of each application and database.
8. Should offer switchover and switchback of individual applications instead of entire system.
9. Any lag in data replication should be clearly visible in dashboard and alerts of same should be sent to respective PFRDA officials.

iii. Data Management

1. Manage data isolation in a multi-tenant environment.
2. Provide tools and mechanism for defining data backup requirements & policy.
3. Provide tools and mechanism for configuring, scheduling, performing, and managing back-ups and restore activities (when required) of all the data including but not limited to files, folders, images, system state, databases, and enterprise applications in an encrypted manner as per the defined policy.
4. Transfer data back in-house either on demand or in case of contract or order termination for any reason, without any additional cost to PFRDA.
5. Manage data remanence throughout the data life cycle.
6. Provide and implement encryption & security mechanisms for handling data at rest and in transit.
7. The SI must implement robust security measures to protect against ransom ware attacks and provide comprehensive incident response plan outlining the steps and procedures in the event of a ransom ware attack.
8. Shall not delete any data at the end of the agreement (for a maximum of 180 days beyond the expiry of the Agreement) without written approval of PFRDA.
9. When SI/CSP (with prior approval of PFRDA) scales down the infrastructure services, SI/CSP is responsible for deleting or otherwise securing PFRDA‘s Content/data prior to VM deletion and in case deleted, shall ensure that the data cannot be forensically recovered.

iv. User/Admin Portal Requirements

Below are the mandatory requirements for all cloud deployment models, but not limited to:

Utilization Monitoring

1. Provide automatic monitoring of resource utilization and other events such as failure of service, degraded service, etc. via service dashboard or other electronic means.
2. Real time performance thresholds
3. Real time performance health checks
4. Real time performance monitoring & Alerts
5. Historical Performance Monitoring
6. Capacity Utilization statistics
7. Cloud Resource Usage including increase/decrease in resources used during auto-scale.
8. Trouble Management –Provide Trouble ticketing via online portal/interface (tools).
9. User Profile Management - Support maintenance of user profiles and present the user with his/her profile at the time of login.

Virtual Machine Requirements

The service shall be available online, on-demand and dynamically scalable up or down as per the requirements of this RFP with two factor authentications via the SSL through a web browser.

1. Service shall provide auto-scalable, redundant, dynamic computing capabilities or virtual machines.
2. Perform an Image backup of VM Image information or support the ability to take an existing running instance or a copy of an instance and export the instance into PFRDA's approved image format.
3. In case of suspension of a running VM, the VM shall still be available for reactivation for a reasonable time without having to reinstall or reconfigure the VM for PFRDA solution. In case of suspension beyond a reasonable time, all the data within it shall be immediately deleted/ destroyed and certify the VM and data destruction to PFRDA as per stipulations and shall ensure that the data cannot be forensically recovered.
4. SI shall ensure that VMs receive OS patching, health checking, Systematic Attack Detection, and backup functions.
5. Monitor VM up/down status and resource utilization such as RAM, CPU, Disk, IOPS and network.
6. Provide services or software based virtual load balancer Services (VLBS) through a secure, hardened, Virtual Load Balancer platform.
7. Provide services or software based virtual load balancing as a service to provide stateful failover and enable Customers to distribute traffic load across multiple servers.
8. Support Clustering
9. Operating System (OS)
    a. Service shall support one or more of the major enterprise grade OS.

b. Management of the OS processes and log files including security logs retained in guest VMs.
c. Provide anti-virus protection.
d. Provide OS level security as per standard operational procedures.

10. Persistence –
    a. Persistent Bundled Storage is retained when the virtual machine instance is stopped or
    b. Non-Persistence – Non-Persistence Bundled Storage is released when the virtual instance is stopped. If quoting Non-Persistence VM, CSP shall provide VM Block storage.
11. RAM (Random Access Memory): Memory (RAM) requirement should be different for different type of servers such as web servers and database servers. VCPU and RAM ratio should be proportionate.
12. Disk Space options allocated for all virtual machines and file data supporting a minimum of 40GB bundled storage.
13. Virtual Machine Block Storage Service Requirements - Service shall provide scalable, redundant, dynamic Web-based storage.
    a. Service shall provide SI with the ability to procure and provision block storage capabilities for cloud virtual machines remotely with two factor authentication via the SSL through a web browser.
    b. Service shall provide block storage capabilities on-demand, dynamically scalable per request for virtual machine instances.
    c. Block Storage – Once mounted, the block storage should appear to the virtual machine like any other disk.
    d. Input/output (I/O) Requests: Input/output requests on block storage
14. PFRDA retains ownership of all virtual machines, templates, clones, and scripts/applications created for its applications.
15. PFRDA retains the right to request full copies of these virtual machines at any time.
16. Support a secure administration interface – such as SSL/TLS or SSH – for SI/PFRDA designated personnel to remotely administer their virtual instance.
17. Provide the capability to dynamically allocate virtual machines based on load, with no service interruption.
18. Provide the capability to copy or clone virtual machines for archiving, troubleshooting, and testing.
19. Cloud provider should offer fine-grained access controls including role-based access control, use of SSL certificates, or authentication with a multi-factor authentication.
20. Cloud service should support auditing with features such as what request was made, the source IP address from which the request was made, who made the request, when it was made, and so on.

21. PFRDA should be permitted to bring and upload additional properly licensed non-operating system software for operation in cloud as required for PFRDA solution for use within the Services by installing it directly on a VM for any Integration.
22. RAM or CPU of virtual machine should scale automatically whenever there is spike in load to deliver application availability even during spike in load.
23. Provide facility to configure virtual machine of required vCPU, RAM, and Disk.
24. Provide facility to use different types of disks like SAS, SSD based on type of application.

Cloud Storage Requirements

1. The service shall be available online, on-demand, and dynamically scalable up or down per request for service from the end users with two factor authentications via the SSL through a web browser.
2. Service shall provide scalable, redundant, dynamic storage.
3. Service shall provide storage capabilities on-demand, dynamically scalable per request and management of the storage.
4. Data Transfer Bandwidth: Bandwidth utilized to transfer files/objects in/out of the providers infrastructure supporting a minimum of Ten (10) GB of data transferred (in and out) within 1 hour via the network.

v. Cloud capacity management workshop

The SI shall conduct training sessions, explaining features of the Cloud system and how to use these features for in case of any departmental requirement. The training material (master copy) will be provided by the solution provider. Hands on training sessions should be of about one day duration and shall be conducted. The training shall be provided by a trained & experienced professional having excellent communication skills. PFRDA will be providing desktops/necessary infrastructure to trainers. The training should be at no extra cost to PFRDA. Bidder will submit two hard copies of the orientation and technical training to PFRDA.

#	Type of Training	Target Audience	No. of sessions	Minimum Duration per Session	Manual/ Material Required
1	Technical Session	PFRDA Officials	Once in every 6 months, for initial two years. Thereafter for any change in the c-panel/tools.	2 Days	Yes

vi. Security Requirements

1. CSP is responsible for provisioning, securing, monitoring, and maintaining the services, network(s), and software that support the infrastructure.
2. In case, CSP provides some of the System Software as a Service (SaaS) for the project, such software to be cloud agnostic.
3. The Data Centre Facility should implement the security tools on the following aspects but not limited to: - Security & Data Privacy (Data & Network Security including Anti-Virus, Virtual Firewall, Multi Factor authentication, VPN, IPS, Log Analyzer/Syslog, SSL, DDOS Protection, HIDS/NIDS, Rights Management, SIEM, Integrated Vulnerability Assessment, SOC, Private Virtual Zones, Data Privacy, Data Encryption, Certifications & Compliance, Authentication & Authorization, and Auditing & Accounting)
4. Meet the ever-evolving security requirements as specified by CERT-In (http://www.cert- in.org.in/)
5. Meet any security requirements published (or to be published) by MeitY or any standards body setup/recognized by Government of India from time to time and notified to CSP by MeitY as a mandatory standard. Security reports for PFRDA setup may be verified by PFRDA anytime, if required.
6. Implement industry standard storage strategies and controls for securing data in the Storage Area Network so that clients are restricted to their allocated storage.
7. Cloud offering should have built-in user-level controls and administrator logs for transparency and audit control.
8. Cloud Platform should be protected by fully managed Intrusion detection system using signature, protocol, and anomaly-based inspection thus providing network intrusion detection monitoring.
9. Cloud platform should provide Edge-to-Edge security, visibility and carrier-class threat management and remediation against security hazards like Denial of Service (DoS) and Distributed Denial of Service (DdoS) attacks, botnets, etc. Also, shall provide protection against network issues such as traffic and routing instability.
10. Cloud platform should provide Web Application Filter for OWASP Top 10 protection as a service that can be enabled for PFRDA that require such a service.
11. Cloud Service provider shall allow audits of all administrator activities performed by PFRDA and allow PFRDA to download copies of these logs in CSV format.
12. Maintain the security features to investigate incidents detected, undertake corrective action, and report to PFRDA as appropriate.
13. Deploy and update commercial anti-malware tools, investigate incidents, and undertake remedial action necessary to restore servers and operating systems to operation.
14. Shall provide consolidated view of the availability, integrity, and consistency of the Web/App/DB tiers.

15. CSP should enforce password policies (complex password, change password in some days etc.)
16. Shall follow PFRDA guidelines and CERT-In Security guidelines. Where there are no procedural guides, use generally accepted industry best practices for IT security.
17. PFRDA has the right to perform audits, scans, reviews, or other inspections of CSPs IT environment for PFRDA that is being used to provide or facilitate services for PFRDA through a MeitY empanelled third party auditor.
18. SI shall be responsible for the following privacy and security safeguards.
19. SI shall not publish or disclose in any manner, without PFRDA's written consent, the details of any safeguards either designed or developed for PFRDA.
20. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of any data collected and stored by SI, CSP/SI shall afford the logical access to the online administration console, monitoring tools, audit logs within 72 hours of the request. Automated audits shall include, but are not limited to, the following methods:
    a. Authenticated and unauthenticated operating system/network vulnerability scans
    b. Authenticated and unauthenticated web application vulnerability scans
    c. Authenticated and unauthenticated database application vulnerability scans

vii. Testing Requirements for CSP

Following cloud resource deployment/provisioning, the testing of the same at Cloud site becomes very important. Therefore, SI must perform following testing:

1. Infrastructure testing – SI should perform various testing procedures listed below on infrastructure (server, storage, and network infrastructure) provided at Cloud site.
    a. VM testing.
    b. Storage/Disk IO testing
    c. Network throughput testing
    d. CPU and RAM benchmarking testing
    e. Read/Write latency testing.
2. Data Integrity Testing, Reverse Replication Testing and Switch over testing: The Cloud service provider will facilitate to carry out these testing, whenever required.

viii. Server Monitoring, Administration

The activities shall include:

1. Configuration of server parameters, operating systems administration and tuning.

2. Operating system administration, including but not limited to management of users, processes, resource contention, preventive maintenance, and management of updates & patches to ensure that the system is properly updated, with minimum or no downtime.
3. Re-installation in the event of system crash/failures.
4. Maintenance of a log of the performance monitoring of servers including but not limited to monitoring CPU, disk space, memory utilization, I/O utilization, etc.
5. Event log analysis generated in all the sub systems including but not limited to servers, operating systems, applications, etc. Ensuring that the logs are backed up and truncated at regular intervals.
6. Periodic health check of the systems (covering all cloud resources offered.), troubleshooting problems, analysing, and implementing rectification measures.
7. At any point of time of the contract if, it is found that CSP fails to meet the guidelines & standards as set by GoI within the timeframe set by MeitY, PFRDA reserves the right to instruct SI to replace & appoint new CSP with approval of PFRDA. The new CSP should have all the technical competencies and capabilities to fulfil requirements as given for this project to meet the required Government guidelines and standards. PFRDA will not bear any additional cost for this activity.

ix. **Reports**

a) Daily reports

1. Summary of issues/complaints logged at the Help Desk
2. Summary of resolved unresolved and escalated issues/complaints.
3. Summary of resolved unresolved and escalated issues/complaints to vendors.
4. Log of backup and restoration undertaken.

b) Weekly Reports

1. Summary of systems rebooted.
2. Summary of issues/complaints logged with the OEMs.
3. Summary of changes undertaken in the Data Centre with respect to PFRDA setup including major changes like configuration changes, patch upgrades, etc. and minor changes like log truncation, volume expansion, user
4. Creation, user password reset, etc.
5. Report for Security Breaches if any and action taken by CSP.
6. Patch update status of all servers including the Virtual Machines running on in

c) Monthly reports

1. Component wise server as well as Virtual machines availability and resource utilization
2. Consolidated SLA/(non)- conformance report.

3. Summary of component wise uptime.
4. Log of preventive/scheduled maintenance undertaken
5. Log of break-fix maintenance undertaken
6. All relevant reports required for calculation of SLAs.

d) Quarterly Reports

1. Consolidated component-wise availability and resource utilization.
2. All relevant reports required for calculation of SLAs.
3. The MIS reports shall be in-line with the SLAs and the same shall be scrutinized by PFRDA.
4. The cloud service provider will also provide any other report requested by PFRDA or any other agency approved and authorized by PFRDA.

x. Security Audit

The Cloud Service Provider's services offerings shall comply with the audit requirements defined under the terms and conditions of the empanelment as per MEITY guidelines as and when published.

The SI shall conduct vulnerability and penetration test from a third-party CERT-IN empanelled agency on the Cloud solution annually and reports should be shared at the cost of SI. SI needs to update the system in response to any adverse findings in the report, without any additional cost to PFRDA. PFRDA may also depute auditors to conduct security check/vulnerability test/penetration test. Additionally, the SI shall ensure all newly deployed Infrastructure is in compliant with all applicable regulatory requirements.

xi. Additional Roles and Responsibilities of SI with respect to cloud

1. SI to provide best Services sizing for this project along with the other products.
2. SI shall develop, prepare, and provide a Cloud Solution Implementation Plan. The Implementation Plan shall have the detailed design, specifications, drawings, and schedule along with inspection and test plan, risk matrix and risk mitigation strategy, training material and documentation for all deliverables.
3. The SI will be responsible for commissioning the appropriate bandwidth, for smooth replication of data.
4. The solution is envisaged for application-level recovery scalable to site level recovery based on the impact of the disaster.
5. Ensuring related DNS changes for internet, application availability and integrity, and database synchronization with application at DR site.
6. Monitoring and maintenance reports over a monthly basis and as and when required.
7. Availability of server logs/records for audits

8. Access to monitoring tools for measuring the service levels, application performance, server performance, storage performance and network performance.
9. Support in audit of the entire system on yearly basis
10. On expiration/termination of the contract, handover of complete data in the desired format to PFRDA which can be easily accessible and retrievable.
11. Reverse Replication is necessary and envisaged when the DR setup is acting as the main setup. The solution should ensure consistency of data in reverse replication till the operations are not being established at the Cloud setup. The RPO would be applicable in reverse replication also. The entire data should be made available for restoration at Primary Data Centre. Restoration at Primary Data Centre will be the prime responsibility of SI. SI to ensure that backup data format to be restorable at Cloud setup or DR setup.
12. Detailed RACI matrix for the same is to be provided by SI.

xii. Application Performance Management (APM) tool & SLA monitoring tool

SI to provide an enterprise grade APM tool & SLA monitoring tool to PFRDA & submit reports from the tool to PFRDA at time to time & on need basis for but not limited to:

1. Real-time monitoring to track application performance.
2. End-to-end visibility into the application stack.
3. Root cause analysis for quick issue resolution.
4. Customizable alert configurations for performance monitoring.
5. Efficient resource utilization.
6. Comprehensive reporting and analytics.
7. Integration with existing monitoring and management tools.
8. Robust security and compliance features to safeguard our applications and data.
9. Various SLA monitoring mechanisms as defined in the SLA section – needed by PFRDA.

42. Waiver of Rights

Each Party agrees that any delay or omission on the part of the other Party to exercise any right, power or remedy under this RFP will not automatically operate as a waiver of such right, power or remedy or any other right, power or remedy and no waiver will be effective unless it is in writing and signed by the waiving Party. Further the waiver or Single or partial exercise of any right, power, or remedy by either Party hereunder on one occasion will not be construed as a bar to a waiver of any successive or other right, power, or remedy on any other occasion.

43. Liquidated Damages (LD)/Compensation for Delay

If SI fails to deliver any or all of the Service(s)/Systems or perform the Services within the time period(s) specified in the RFP/Contract/Agreement, PFRDA shall, without prejudice to its other rights and remedies under and in accordance with the RFP/Contract/Agreement, levy Liquidated Damages (LD) from payments, which are due to the SI.

For calculation of LD:

1. LD for delay in the Service(s) rendered for each month of delay beyond the scheduled date or part thereof will be a sum equivalent to 1.0% of total cost of the project (TCO) per month. The overall LD will be maximum of 10% of the total cost of the project. After attaining the maximum Compensation of 10% of total project cost/TCO , PFRDA may consider termination of the contract.
2. PFRDA reserves its right to recover compensation amount by any mode such as adjusting from any payments to be made by PFRDA to SI.
3. PFRDA may, at its discretion, waive the liquidated damages in case the delay may not be attributable to SI.
4. Any such recovery or liquidated damages shall not in any way relieve the SI from any of its obligations to complete the works/service(s) or from any other obligations and liabilities under the Contract/Agreement.

The compensation will be applicable as mentioned in SLA and compensation - ***Appendix-IV*** of this RFP.

44. General Requirements

1. SI shall provide dedicated resources for PFRDA's project.
2. There should be sufficient headroom (at an overall level in the compute, network and storage capacity offered) available for near real time provisioning during any unanticipated spikes in the user load.
3. Ability to integrate fully with the Government of India approved Certifying Authorities to enable PFRDA to use the Digital Certificates/Digital Signatures.
4. PFRDA shall retain ownership of any user created/loaded data and applications hosted on CSPs infrastructure and maintain the right to request (or should be able to retrieve) full copies of these at any time.
5. PFRDA retains ownership of all templates, clones, and scripts/applications created for PFRDA's application and retains the right to request (or should be able to retrieve) full copies at any time.
6. PFRDA shall be provided access rights (including the underlying secure connection) to the user administration/portal of cloud services to have visibility into the dashboard, SLAs, management reports, etc. provided by the Cloud Service provider.
7. SI will ensure that CSP shall not provision any unmanaged VMs for the applications.

8. SI will ensure that CSP shall provide interoperability support with regards to available APIs, data portability etc. for PFRDA to utilise in case of Change of cloud service provider, migration to different cloud/in-house infrastructure, burst to a different cloud service provider or availing backup or DR services from a different cloud service provider as and when needed.
9. Should adhere to the ever-evolving guidelines as specified by CERT-In (http://www.certin.org.in/)
10. Should adhere to the relevant standards published (or to be published) by Ministry of Electronics & Information Technology (MeitY) or any standards body setup/recognized by Government of India
11. Cloud Infrastructure shall be accessible to PFRDA, or any third party engaged by PFRDA for inspection and audit purposes, if any. Bidders shall also adhere to the relevant audit requirements as defined in the RFP.

I. Compliance

SI shall be responsible to comply with the provisions of PFRDA Act and the Rules and Regulations framed thereunder, and the directions/guidelines/notification/circulars issued by PFRDA from time to time, and any other applicable laws/Rules/Regulations/guidelines in force.

Disputes, if any, arising out of this selection process, shall be subject to the exclusive jurisdiction of Courts at New Delhi only. Post the award of the Contract, the disputes, if any arising thereunder shall be settled in terms of the provisions of the Arbitration and Conciliation Act, 1996, as provided under such Contract.

II. Interpretation

In case of any clarification with regard to the terms used in this RFP and conditions of this RFP, the interpretation of PFRDA, shall be final.

Annexure-I: Covering Bid Form (Technical Bid)

[On Company's letter head] (To be included in Technical Bid)

Date: _

RFP Reference No: PFRDA/2024/TARCH/PFRDA-TRACE/01

To,

Chief General Manager

In charge- PFRDA-TRACE

Pension Fund Regulatory and Development Authority (PFRDA)

B-14/A, Qutab Institutional Area, Chhatrapati Shivaji Bhavan, Katwaria Sarai, New Delhi-110016

Dear Sir,

We have examined the above RFP, the receipt of which is hereby duly acknowledged and subsequent pre-bid clarifications/modifications/revisions, if any, furnished by PFRDA and we offer to supply, Install, test, commission and support the desired Software Solution detailed in this RFP. We shall abide by the terms and conditions spelt out in the RFP. We shall participate and submit the Bid.

While submitting this Bid, we certify that:

1. All information provided in the Proposal and in the Appendices to it is true and correct and the documents accompanying such Proposal are in original or true copies of their respective originals.
2. This statement is made for the express purpose of qualifying as a SI for System design, develop, Implementation and its Maintenance for the time duration as given in this RFP.
3. We are in existence and operational for the last five complete financial years.
4. The undersigned is authorized to sign on behalf of the bidder and the necessary support document delegating this PFRDA is enclosed to this letter.
5. We declare that we are not in contravention of conflict-of-interest obligation mentioned in this RFP.
6. Prices submitted by us have been arrived at without agreement with any other Bidder of this RFP for the purpose of restricting competition.
7. The Financials submitted by us have not been disclosed and will not be disclosed to any other Bidder or any person connected with any of the bidders responding to this RFP.
8. We have quoted for all the products/services mentioned in this RFP in our Financial Bid.

9. The rate quoted in the Financial Bids are as per the RFP and subsequent pre- Bid clarifications/modifications/revisions furnished by PFRDA, without any exception.
10. We undertake that, in competing for (and, if the award is made to us, in executing) the above contract, we will strictly observe the laws against fraud and corruption that are in force in India including but not limited to "Prevention of Corruption Act 1988".
11. We undertake that we will not offer, directly or through intermediaries, any bribe, gift, consideration, reward, favour, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of PFRDA or members of the bid evaluation committee, connected directly or indirectly with the bidding process, or to any person, organization or third party related to the contract in exchange for any advantage in the bidding, evaluation, contracting and implementation of the contract. We also understand that any violation in this regard, will result in disqualification of bidder from further bidding process.
12. It is further certified that the contents of our Bid are factually correct. We have not sought any deviation to the terms and conditions of the RFP. We also accept that in the event of any information/data/particulars proving to be incorrect, PFRDA will have right to disqualify us from the RFP without prejudice to any other rights available to PFRDA.
13. We certify that while submitting our Bid document, we have not made any changes in the contents of the RFP document, read with its amendments/clarifications provided by PFRDA.
14. We agree to abide by all the RFP terms and conditions, contents of Service Level Agreement as per template available at ***Appendix-IV*** of this RFP and the rates quoted therein for the orders awarded by PFRDA up to the period prescribed in the RFP, which shall remain binding upon us.
15. On successfully being declared as "Successful bidder", we undertake to complete the formalities as specified in this RFP.
16. We understand that PFRDA is not bound to accept any bid received and may reject all or any bid without assigning any reason or giving any explanation whatsoever.
17. We hereby certify that our name does not appear in any "Caution" or ' Black-Listed' list of any regulatory body, Government Authority or Public Sector Undertaking (PSUs) in India or any Financial Institution in India as on date of submission of response.
18. We confirm that we will not sub-contract the assignment/work.
19. We hereby certify that on the date of submission of Bid for this RFP, we do not have any past/present litigation which adversely affect our participation in this RFP, or we are not under any debarment/blacklist period for breach of contract/fraud/corrupt practices by any Scheduled Commercial Bank/Public Sector Undertaking/State or Central Government or their agencies/departments for the time period given in RFP.
20. We hereby certify that OEMs for the different components of the software solution being offered to PFRDA have a fully functional support Centre in India.

21. If our Bid is accepted, we undertake to enter and execute at our cost, when called upon by PFRDA to do so, a contract in the prescribed form and we shall be solely responsible for the due performance of the contract.
22. Bidder and all the proposed OEM/OEMs & CSP partner should not be under debarment/blacklist period for breach of contract/fraud/corrupt practices by any Regulatory bodies/Scheduled Commercial Banks/Public Sector Undertaking/State or Central Government or their agencies/departments during the last three years as on date of submission of the bid.
23. We, further, hereby undertake and agree to abide by all the terms and conditions stipulated by PFRDA in the RFP document.

Dated this ..... day of _____ 2024._____

*(Signature)*_____ *(Name)*_____

(In the capacity of)

Duly authorized to sign Bid for and on behalf of_____

Seal of the company

Annexure-II: BIDDER Details

Details to be filled by bidder.

S. No.	Particulars	Details
a.	Name	
b.	Constitution of the company	
c.	Date of Incorporation and/or commencement of business	
d.	Certificate of incorporation	
e.	Brief description of bidder including details of its main line of business	
f.	Company website URL	
g.	Company PAN	
h.	Company GSTIN	
i.	Company Bank Account Number (to be used for returning EMD)	
j.	Company bank details (Name, Branch, IFSC, etc.)	
k.	Particulars of the Authorized Signatory of bidder Name Designation Address Phone Number (Landline) Mobile Number Fax Number Email Address	

Name & Signature of authorized signatory

Seal of Company

Annexure-III: Financial Capability Statement

(On Statutory Auditor's letterhead)

Date: DD/MM/YYYY

To,

Chief General Manager
In charge- PFRDA-TRACE
Pension Fund Regulatory and Development Authority(PFRDA)
B-14/A, Qutab Institutional Area, Chhatrapati Shivaji Bhavan, Katwaria Sarai, New Delhi-110016

Dear Sir,

I/We hereby declare that I/We have scrutinized and audited the financial statement of M/s_____ . I/We certify that M/s _____is a profitable entity for the last three financial years (i.e. FY 2022-23, FY 2021-22, FY 2020-21) and has not incurred any cash loss during the period.

The Net worth, Profit after tax (PAT), total Turnover, and the Turnover of bidder from IT and IT enabled services (ITeS) for last three Financial years as per audited statement is as under:

	Net worth (INR Crore)	**PAT (INR Crore)**	**Total Turnover (INR Crore)**	**Turnover from IT/ITeS**	**Average Turnover from IT/ITeS for the last 3 financial years i.e., FY (2022- 23, 2021- 22, 2020-21)**
2022-23					
2021-22					
2020-21					

_____

Signed and Sealed by Statutory Auditor

Name:

Designation:

Address:

Telephone & Fax:

E-mail address:

Annexure-IV: Pre-Bid Query Format

(To be provided strictly in Excel format) All the pre-bid queries to be submitted through email (itprojects-pfrda@pfrda.org.in) only by the given due date for submission of queries. In no other way, pre-bid queries will be entertained. Pre-bid queries to be submitted strictly in the format given below:

(To be provide strictly in Excel format)

Vendor Name	Sl. No	RFP Page No	RFP Clause No.	Existing Clause	Query	Suggestions

Name & Signature of authorized signatory

Seal of Company

Annexure-V: Eligibility Criteria

Bidders meeting the following criteria are eligible to submit their Bids along with supporting documents. If the Bid is not accompanied by all the required documents supporting eligibility criteria, the same would be rejected:

Eligibility Criteria	**Description/Requirement**	**Documents to be Submitted**
Legal Entity	a. Bidder should be registered as a Company in India as per the Indian Companies Act, 1956/2013 or a Limited liability Partnership firm registered under the Limited Liability Partnerships Act, 2008. b. Registered with the GST authorities. c. Should have been in existence and operational for the last five complete Financial years.	i. For a & c. - Certificate of Incorporation//LLP Registration and ***Annexure-I*** and ***Annexure-III*** ii. For b - GST registration certificate
Legal Litigation & Blacklisting	Bidder should not be under debarment/blacklist period for breach of contract/fraud/corrupt practices by any Regulatory bodies/ Scheduled Commercial Banks/Public Sector Undertaking/State or Central Government or their agencies/departments during the last three (03) years as on date of submission of the bid.	Bidders should specifically certify in ***Annexure-I*** in this regard.
Experience and Track Record	Bidder must have successfully completed a minimum of one (01) software solution or project as a System Integrator (SI) on or after 01-01-2019 till bid submissions end date of this RFP. This project should be related to Compliance Management and Data Analytics Systems. The qualifying experience should be with Central or State Government, Regulatory Bodies, Central or State Government-owned Organizations, Public Sector Undertakings (PSUs), Autonomous Bodies, Public Sector Banks, Public	(i)Work order + Completion certificates from the client. OR (ii)Work order + Self certificate of completion (Certified by the Authorised Signatory giving details of execution of the project) as per ***Annexure – X*** OR (iii)Project completion Certificate issued by Company's statutory

Eligibility Criteria	Description/Requirement	Documents to be Submitted
	Sector Insurance Companies, Central Public Sector Enterprises (CPSEs), Statutory or Registered Trust dealing with statutory schemes for beneficiaries in India or Corporates having at least 100 users or above in India or abroad. Note: For the purpose of Eligibility criteria and Technical evaluation: i. Compliance Management System means a system/software solution similar to the functional scope of work as mentioned in this RFP such as submission of reports, acceptance/rejection on the submitted reports, alerts, MIS Report generation on selected data points etc. ii. Data Analytics Systems means a system/software solution similar to the functional scope of work as mentioned in this RFP such as generation of Reports, Infographics, Dashboards on selected or all data points, search mechanism etc. iii. Project completed means Project or its relevant phase is Go-live and its acceptance received from the client. In case of non-availability of acceptance letter from the client on completion of the project, PFRDA may ask for Invoice /payment receipt and the corresponding TDS certificate to ascertain project completion status.	auditor/Company Secretary on letterhead giving details of execution of the project as per ***Annexure – X***
Financial Stability	Bidder must have been a profitable entity for the last three Financial years* (i.e., FY 2022-23, FY 2021-22, FY 2020-21) and has not incurred any cash loss during the period.	Audited Financials or Certificate issued by Company's statutory auditor on the Profitability (PAT) and cash loss for the last three Financial years (i.e. FY 2022-

Eligibility Criteria	Description/Requirement	Documents to be Submitted
	*In case, the company/LLP operates on calendar year, the audited statements will be required for calendar years 2020, 2021 and 2022	23, FY 2021-22, FY 2020-21) as per ***Annexure-III***
Financial Stability	Bidder must have an average turnover of Rs. Two Hundred Fifty (250) Crore or above from IT and IT enabled services (ITeS) during the last 03 (three) Financial year(s) (i.e. FY 2022-23, FY 2021-22, FY 2020-21 *In case, the company/LLP operates on calendar year, the audited statements will be required for calendar years 2020, 2021 and 2022	Copy of the audited financial statement for required Financial years. (i.e., FY 2022-23, FY 2021-22, FY 2020-21) as per ***Annexure-III***
Relevant Certifications	Bidder should hold relevant and valid certifications CMMI Level 3 or above, to highlight commitment to quality and process maturity.	CMMI level 3 or above certificate valid as on due date of submission of bid
Eligibility criteria for Cloud Service provider (CSP) to be engaged by SI	Meity empanelled CSP for providing cloud services in the form of GCC/VPC	Certificate/document showcasing that CSP is Meity empanelled as on due date of submission of bid

**All information furnished against each of the above criteria must be supported by valid documents as mentioned above along with index. The authorised signatory of bidder must sign all documents. Relevant portions, in the documents submitted in pursuance of eligibility criteria, should be highlighted. If all these conditions are not fulfilled or supporting documents are not submitted with the technical Bid, then all those Bids will be summarily rejected, and no queries will be entertained.

Name & Signature of authorised signatory

Seal of Company

Annexure-VI: Technical Evaluation Parameters

The bid document will be evaluated as per the requirements specified in the RFP. Bidder is required to submit all required documentation in support of the functional specification criteria specified. Technical presentation will be a part of the process.

Each Technical Bid will be assigned a technical score out of a maximum of 100 marks. Only bidders with overall score of 70 marks or more will be technically qualified and short listed for financial evaluation. Failing to secure minimum marks shall lead to technical disqualification of the Bid.

1. Scoring Model

Bidder's technical proposal will be evaluated as per the requirements specified in the RFP and adopting the following evaluation criteria.

Section	Evaluation Criteria	Total Marks Awardable
A	Understanding of PFRDA's requirement and proposed solution architecture	22
B	Bidders experience according to PFRDA's Functional and Technical Requirement Specifications	14
C	Client References	16
D	Bidders' relevant key manpower capability	10
E	Relevant Project Experience	12
F	Product Walk Through	16
G	CMMI Compliance & ISO Assessment	10
	Total	***100***

The detailed scoring model is given below –

A. Understanding of PFRDA's requirement and proposed solution architecture (Max marks: 22)

Within this section, a maximum of 22 marks is assigned to ascertain bidders' capability based on their demonstrated understanding of PFRDA project requirements and proposed solution architecture.

These criteria would be assessed based on technical proposal, & presentation given by the bidder.

A	Evaluation Criteria		Total Maximum Marks Awardable
A	Bidders must demonstrate their understanding of the requirements by providing a clear description of the Scope of Work, proposed solution and its fitment factor, tailored according to PFRDA business requirements. The following components shall be covered:	**Max. Marks Awardable**	22
i.	Understanding of PFRDA requirements as per Scope of work	2	
ii.	Implementation Approach and Methodology	2	
iii.	Experience in proposed Technology Stack	2	
iv.	Project plan	2	
v.	Cyber Security Methodologies	2	
vi.	In-depth analysis of challenges and opportunities in the project implementation	1	
vii	Clear articulation on how the proposed solution address requirements of the scope of work	1	
viii	Post Implementation support and services	1	
ix	Relevant cloud experience	1	
x.	Stability, scalability of the proposed solution	2	
xi.	Demonstrated awareness of Industry best practices for similar kind of projects	1	
xii.	Exit plan including Cloud port out plan	1	
xiii.	PFRDA-TRACE Roadmap and Business Continuity	2	
xvi.	Technical Presentation covering salient aspects of the project with Content and Information clarity	2	
	Total	**22**	

B. Bidders experience according to PFRDA's Functional and Technical Requirement Specifications (Max. marks: 14)

Bidder's experience for project implemented on or after 01-01-2019 till bid submissions end date of this RFP should be congruent with PFRDA's specifications, contributing to the overall score in the technical proposal assessment. Maximum Fourteen (14) marks will be assigned to evaluate bidder's experience in alignment with PFRDA's Functional and Technical Requirement Specifications, focusing on essential criteria such as the automated dissemination of email alerts, notifications, and reports to stakeholders, role configuration, privilege management, anomaly detection, electronic and digital signature integration, adaptability to external system interfaces through APIs, flexibility for future user role onboarding, proficiency in processing extensive datasets with enterprise-level business intelligence tools, and the capacity to uncover intricate data connections.

This criterion would be assessed based on technical proposal, presentation & ***Annexure- XVII*** *submitted by the bidder.* PFRDA reserves the right to cross check & verify any/all of the submitted experiences & references via email, call, visit, ask for submission of relevant Invoice/Payment receipt with corresponding TDS certificate, Workorder or any other possible modes, at PFRDA's discretion.

B	Evaluation Criteria	Max. Marks Awardable	Total Maximum Marks Awardable
i.	The implemented solution should be able to send out automated emails alerts notifications, reports to all/defined stake holders.	2	14
ii.	The implemented solution should have features of configuring roles, privileges & access management-based control.	2	
iii.	The implemented solution should use rule engine for detecting anomalies & raise flags as required by PFRDA.	2	
iv.	The implemented solution should be capable of integration with electronic and digital signature capabilities.	2	
v.	The implemented solution should be able to integrate with systems of external organizations through APIs & other modes. The solution should be flexible so that any new user role could be on boarded in future.	2	
vi.	The implemented solution should be able to create basic workflows like adding new	2	

B	Evaluation Criteria	Max. Marks Awardable	Total Maximum Marks Awardable
	compliance reports, assign it to user groups, add relevant section in old reports or create new reports - by user department/PFRDA Admin.		
vii	The implemented solution should be able to create web forms, assign them to user groups under category & subcategory - by user department/PFRDA Admin.	2	
	Total	**14**	

C. Client References (Max marks: 16)

This section is to evaluate bidder's relevant experience, ensuring that their technology stack, use cases, and project engagement align with PFRDA's project requirements. To assess Bidder's Proven Relevant Experience, this evaluation will draw insights from two provided customer references where the bidder as SI has implemented on or after 01-01-2019 till bid submissions end date of this RFP. Each reference will be scrutinized based on the following criteria:

1. Demonstrated Relevance (4 Marks):
    a. Maximum two (02)marks will be assigned for the alignment of the technology stack utilized in the reference project with the specifications of our proposed solution.
    b. An additional two (02) marks will be granted for showcasing use cases that closely mirror the intricacies of the proposed PFRDA-TRACE.
2. Project Engagement Nature (04 Marks):
    a. A full four (04) marks will be awarded if the reference highlights both the successful implementation of the project and continued/continuing support, underscoring bidder's comprehensive project management capabilities.
    b. Should the reference predominantly focus on the implementation phase, a rating of 2 marks will be assigned, recognizing the ability to initiate projects effectively.
    c. In the event that the reference primarily emphasizes only support services, a score of 2 marks will be designated, acknowledging bidder's proficiency in offering ongoing maintenance and assistance.

** to fulfil this criteria bidder needs to showcase relevant experience for each project detail in the format given in ***Annexure-X***. PFRDA reserves the right to cross check & verify any/all of the submitted experiences & references via email, call, visit, ask for relevant Invoice submitted/

payment receipt with corresponding TDS certificate or any other possible modes, at PFRDA's discretion.

C	Evaluation Criteria			Total Maximum Marks Awardable
	Client references of Relevant Experience Marks are indicated per client reference. Client references (02) should include:	**Marks awardable**	**Max. Marks Awardable**	16 (08 marks for each client)
C.1	(i) Relevant experience (For each project)		8	
	(a) Similarity of technology stack	2		
	(b) Use cases like proposed PFRDA-TRACE	2		
C.2	(ii) Nature of project (For each Project)		8	
	(a) Implementation & Support both	4		
	(b) Only Implementation	2		
	(c) Only Support	2		
	Total		**16**	

D. Bidders' relevant key manpower capability (10 marks)

In this section the evaluation of Bidders' relevant manpower capability, weighing ten (10) marks, will be carried out with a focus on the proposed workforce and their alignment with previous experience akin to the project at hand. Each bidder's proposed manpower will be scrutinized for their expertise and experience in fields closely related to the project requirements. A key emphasis will be placed on the relevance of their previous experience to the specific needs of our project, ensuring that the manpower possesses the skills and knowledge necessary for its successful execution. This evaluation is paramount in determining bidder's capacity to assemble a competent team capable of meeting the project's demands effectively. While submitting the bid the bidder shall certify on bidders' letterhead that the proposed key manpower for this project is having the relevant experience & the relevant academic qualifications.

Bidders to note that the proposed role of the candidate should be mentioned clearly on top of the resume. One candidate should not be proposed for multiple roles. Additional CVs could also be recommended by the bidder to showcase capability but the same should not be carrying

any extra marks in the evaluation. The bidder in this case is recommended to mention 'Additional profile for Role – XXXX' on top of the resume. In the case of any ambiguity (if the bidder mentions multiple candidates for a single role, scoring will be calculated based on the candidate with minimum experience during the evaluation.

Each resume submitted by the bidder must also bear the signature of the proposed key manpower. The key manpower should be same at the time of project implementation as proposed in bidder's technical proposal. If, due to unforeseen circumstances, there are changes in manpower, the bidder must ensure that any newly proposed key personnel possess equal or greater relevant experience and qualification. In case any manpower is not performing as per the satisfaction of PFRDA, the bidder shall replace the concerned manpower to the satisfaction of PFRDA.

D	**Proposed Project Team**				**Max Marks Awardable**
		With Experience relevant to PFRDA-TRACE			**10**
	Role	**=>7 years**	**5-7 years**	**<5 years**	**Max. Marks Awardable**
i.	Project Manager	2	1	0	2
ii.	Business Analyst	1	0.5	0	1
iii.	Solution Architect	2	1	0	2
iv.	Data Scientist/ Data Architect	1	0.5	0	1
v.	Cyber Security Expert	1	0.5	0	1
vi.	Subject Matter Expert	2	1	0	2
vii	Data Presentation/ Visualization Expert	1	0.5	0	1
		10	5	0	10

Resumes of the key manpower nominated by bidder for this project needs to be submitted in the prescribed format as mentioned in ***Annexure-XVI.***

E. Relevant Project Experience (12 Marks)

Any bidder with a proven track record in successfully implementing (go live) software solution(s) or project(s), particularly as a System Integrator (SI), related to Compliance Management System and Data Analytics Systems will be considered for project completed on or after 01-01-2019 till bid submissions end date of this RFP. Evaluation of the bidder's experience will focus on the effective implementation of the similar components/modules.

The qualifying experience must be affiliated with entities such as Central or State Government, Regulatory Bodies, Central or State Government-owned Organizations, Public Sector Undertakings (PSUs), Autonomous Bodies, Public Sector Banks, Public Sector Insurance Companies, Central Public Sector Enterprises (CPSEs), Statutory or Registered Trust dealing with statutory schemes for beneficiaries in India or Corporates having at least 100 users or above, either within India or abroad. Project Cost should be exclusive of GST.

PFRDA reserves the right to cross check & verify any/all of the submitted experiences & references via email, call, visit, ask for relevant Invoice submitted/ payment receipt and corresponding TDS certificate or any other possible modes, at PFRDA's discretion.

No of projects	Project(s) Cost (Rs 02-05 Crore)	Project(s) Cost (Rs 05-15 Crore)	Project cost (above Rs 15 Crore)	Max marks Awardable
One project	1 mark	2 marks	4 marks	12
Two Projects	2 marks	4 marks	8 marks	
Three Projects & more	3 marks	6 marks	12 marks	

F. Product walkthrough (16 marks)

Within this segment, a maximum of sixteen (16) marks is designated to gauge bidders' proficiency in delivering a robust Compliance Workflow management, BI & Analytics, Data Management, MIS, and Dashboard solution. The bidder is required to demonstrate the live product(s) view (Application's live view – no presentation or wireframing) focusing on features as per the SoW. The product demonstration may be done with dummy data, workflow, MIS, dashboards. Marks will be specifically allocated to assess the proposed solution's capabilities and architecture. This includes a thorough examination of the solution's innovation, scalability, and alignment with our organization's unique requirements, focusing on key areas such as the coherence and efficiency of the proposed solution architecture, the effectiveness and compatibility of integrated solutions, cybersecurity methodologies, implementation approach, and the relevance of the technology stack.

F	Evaluation Criteria	Max Marks:	Max Marks
1	Product Capability & flexibility in custom configuration	5	**16**
2	Similar Features Availability	4	
3	Scalability	2	
4	User-Friendly Interface	2	
5	Product Roadmap	3	
	Total	**16**	

G. Certifications of the SI & CSP (10 marks)

Within this section, a total of ten (10) marks is dedicated to evaluating bidders' adherence to Capability Maturity Model Integration (CMMI) levels 5, as well as ISO 9001 and ISO 27001 standards. Four (04) marks specifically assess the bidder's alignment with CMMI level 5 standards, emphasizing continuous improvement and organizational excellence. Additionally, Two (02) marks each are allocated for adherence to both ISO 9001 and ISO 27001 standards, recognizing the establishment of a quality management system and commitment to information security management. Bidders are encouraged to substantiate their claims with evidence, certifications, or case studies showcasing successful implementations, influencing their overall score in this section, and demonstrating a comprehensive commitment to quality, process maturity, and information security.

If the cloud service provider is having SOC 3 Two (02) marks are allocated for the same.

Note: The marking of the parameters is mentioned on the maximum basis. However the Bid Evaluation Committee may give less marks even in decimal points, for evaluation of the bids based on qualitative parameters proposed in the bid.

Annexure-VII: Manufacturer's Authorisation Form (MAF) by Original Equipment Manufacturer (OEM)

Indicative MAF as given below – all OEMs whose products are factored in the proposed solution needs to share their MAF acceptable to PFRDA/in the format as mentioned below.

[On the Letter head of OEM]

Date:

To,
Chief General Manager
In charge- PFRDA-TRACE
PENSION FUND REGULATORY AND DEVELOPMENT AUTHORITY(PFRDA)
B-14/A, Qutab Institutional Area, Chhatrapati Shivaji Bhavan, Katwaria Sarai, New Delhi-110016

Dear Sir,

Ref.: Authorization letter from OEM to ----- (Bidder) for participation in bid for RFP Reference No: PFRDA/2024/TARCH/PFRDA-TRACE/01

Particular	**Original Supplier/make & model/development/ Unit details**
Software Licences including	
Core Solution	
<<Please insert details as required>>	
Other *(Please insert other Components, as required)*	

We hereby extend our full guarantee and comprehensive warranty as per terms and conditions of the tender and the contract for our equipment quoted/services offered against this invitation for Bid by the above company/LLP.

We undertake to deliver the services as mentioned in the scope of work of RFP for OEM and hereby extend our warranty/support and services through M/s……during the … years contract period as per terms and conditions of the RFP.

We also undertake that we have not been under debarment/blacklist period for breach of contract/fraud/corrupt practices by any Regulatory bodies/ Scheduled Commercial

Banks/Public Sector Undertaking/State or Central Government or their agencies/departments during the last three (03) years as on date of submission of the bid.

The quoted product is of the latest model/version and extends our back-to-back support during the entire duration of Agreement. If any product is found to be obsolete/end of support/end of life during the contract period, we will replace the same with the latest product with the equivalent/higher capabilities for free of cost.

Dated at _____ this _____ day of _____<YEAR>.

Yours faithfully,

[Signature of Authorised Representative of OEM/partner of OEM] [Title] [Organization stamp/seal] [Date]

Annexure-VIII: Financial Bid

Date:

To,
Chief General Manager
In charge- PFRDA-TRACE
PENSION FUND REGULATORY AND DEVELOPMENT AUTHORITY(PFRDA)
B-14/A, Qutab Institutional Area, Chhatrapati Shivaji Bhavan, Katwaria Sarai, New Delhi-110016

Sub: Submission of Financial Bid for DESIGN, DEVELOPMENT, IMPLEMENTATION AND MAINTENANCE OF PFRDA-TRACE (PFRDA - TRACKING REPORTING ANALYTICS & COMPLIANCE e-PLATFORM)

Dear Sir,

Having examined the Bidding Documents, the receipt of which is hereby duly acknowledged, we, the undersigned, offer to design, develop, implement, and maintain the subject mentioned project, in conformity with the said Bidding documents.

1. If our bid is accepted, we undertake to design, develop, implement, and maintain the project in accordance with the delivery schedule specified in this RFP.
2. If our Bid is accepted, we will obtain the guarantee of a bank/Account payee Demand Draft/Fixed Deposit Receipt - issued by a Scheduled Commercial bank - in a sum equivalent to prescribed percent for the due performance of the Contract in the manner prescribed by PFRDA at ***Appendix- II***.
3. We agree to abide by the Bid and the rates quoted therein for the orders awarded by PFRDA up to the period prescribed in the Bid which shall remain binding upon us.
4. We undertake that, in competing for (and, if the award is made to us, in executing) the above contract, we will strictly observe the laws against fraud and corruption in force in India namely including but not limited to "Prevention of Corruption Act 1988".
5. We understand that you are not bound to accept any Bid you may receive.
6. Values in **Table 2** are Year wise details(break-up) of bid price for the purpose of record and reference only (to be matched with Total cost of Project **(TCO)).**

Bidders to note that:

1. Prices to be filled in Table 1 wherever applicable.
2. Unit price shall be quoted wherever applicable.
3. Bidder should clearly specify make and version of the items wherever applicable.
4. Prices quoted must be firm till the completion of the contract including Warranty & Support period.

5. The financial bid should also include service charge or any additional payment including Bidder's profit, bonus, insurance, engineer support charges etc. made for supporting the system.

Dear Sir,

Ref.: Your RFP Reference No: PFRDA/2024/TARCH/PFRDA-TRACE/01

Detailed 'Financial Bid' with List of Products, Solutions, Services and Licences

Please mention 'Not Applicable'/NA wherever price is not quoted for the particular cell.

S. no.	Phase & Tenure	Section	Item	Cost in INR (Excl GST)	Total Cost in INR Excl GST in words	Cost in INR (Incl GST)	Total Cost in INR Incl GST in words
A	**Development Phase Duration - 1 year**	A.1	Application Development Cost				
		A.2	Security Audit & VAPT Cost				
		A.3	Training Cost with Training Materials				
		A.4	Any other cost (mention item details in subsequent rows) I II III ….	-		-	
	(A) Total Cost for Development Phase						
B	**License Cost**	B.1	License Cost for Development Phase				
		B.2	License /Subscription Cost for Warranty & Stabilization Phase				
		B.3	License /Subscription Cost for 1st year AMC				
		B.4	License /Subscription Cost for 2nd year AMC				
		B.5	License /Subscription Cost for 3rd year AMC				
		B.6	License /Subscription Cost for 4th year AMC				
	(B) Total Cost for License Cost						
C	**Warranty & Stabilization Phase** **Duration - 1 year**	C.1	Cloud Cost				
		C.2	Technical Helpdesk				
		C.3	Facility Management cost including manpower				
		C.4	Warranty & Stabilization cost for one Year				
		C.5	Any other cost (mention item details in subsequent rows) I II III ….				
	(C) Total Cost for Warranty & Stabilization Phase						
D	**AMC Phase Year 1**	D.1	Cloud Cost				
		D.2	Technical Helpdesk				

S. no.	Phase & Tenure	Section	Item	Cost in INR (Excl GST)	Total Cost in INR Excl GST in words	Cost in INR (Incl GST)	Total Cost in INR Incl GST in words
		D.3	AMC cost				
		D.4	Any other cost (mention item details in subsequent rows) I II III ….				
	(D) Total Cost for first year AMC						
E	**AMC Phase Year 2**	E.1	Cloud Cost				
		E.2	Technical Helpdesk				
		E.3	AMC cost				
		E.4	Any other cost (mention item details in subsequent rows) I II III ….				
	(E) Total Cost for second year AMC						
F	**AMC Phase Year 3**	F.1	Cloud Cost				
		F.2	Technical Helpdesk				
		F.3	AMC cost				
		F.4	Any other cost (mention item details in subsequent rows) I II III ….				
	(F) Total Cost for third year AMC						
G	**AMC Phase Year 4**	G.1	Cloud Cost				
		G.2	Technical Helpdesk				
		G.3	AMC cost				
		G.4	Any other cost (mention item details in subsequent rows) I II III ….				
	(G) Total Cost for fourth year AMC						
H	**(H) Total cost 500-man days of change request**						
I	**I = (D + E + F + G) Total Cost for AMC Phase**						
TCO	**TCO = (A + B + C + H + I) Total Project Cost (Development Phase + Warranty & Stabilization Phase + AMC Phase + 500-man days cost)** *Bid will be evaluated on TCO - exclusive of GST*						

(Unit: in Rs)

Note:

(Signature)

(Name) (in the capacity of)

Duly authorised to sign Bid for and on behalf of

Company Seal

Table-2: Year wise details (break-up) of Price bid/Financial bid

Sr. no.	Particulars	Year	Cost (in Rs.) exclusive of GST as applicable	GST as applicable	Cost (in Rs.) inclusive of GST as applicable
1	Project Cost	1			
2	Project Cost	2			
3	Project Cost	3			
4	Project Cost	4			
5	Project Cost	5			
6	Project Cost	6			
7	Change request man days cost	-			
Total Project Cost (Add sr. no. 1 to 7) to be matched with TCO as bid Financial quoted in Table-1			**Total of sr. no. 1 to 7 exclusives of GST** **In figure: Rs** **_____** **In words: Rs.** **_____**		**Total of sr. no. 1 to 7 inclusive of GST** **In figure: Rs.** **_____** **In words: Rs.** **_____**

(Signature)

(Name) (in the capacity of)

Duly authorised to sign Bid for and on behalf of

Company Seal

Yours faithfully,

[Signature of Authorised Representative of SI]

[Title]

[Organization stamp/seal]

[Date]

Annexure-IX: Payment Milestones

a) Delivery Schedule

1. The total duration for the project will be of six (06) years comprising of Twelve (12) months of development and implementation period (Go-live) from the date of the award of the contract, Twelve (12) months of warranty & stabilization and AMC for Forty-Eight (48) months.
2. During the term of the development phase, no license costs shall be incurred by PFRDA. All license costs associated with the software shall be payable in advance at the beginning of each calendar year. Upon successful implementation and the system's go live, PFRDA shall commence payment for the applicable license costs, which will be billed accordingly.

b) Payment Terms

The payment will be made within 30 days on receipt of proper invoice (original) against successfully completion of the services as per the timeline indicated.

Section	Milestone Number	Payment Milestones	% Payment of Sub-total for Services Provided	Payment frequency for the year
A	**(A) Development phase**			
	1	Project Kick-off, system study & SRS signoff and its acceptance by PFRDA	25% of the cost quoted for development of the application phase as quoted in ***Annexure-VIII*** for the section "Financial Bid" in section “A” mentioned as - Total Cost for Development Phase	1
	2	UAT Signoff and its acceptance by PFRDA	25% of the cost quoted for development of the application phase as quoted in ***Annexure-VIII*** for the section "Financial Bid" in section “A” mentioned as - Total Cost for Development Phase	1
	3	Audit (security & VAPT) and its acceptance by PFRDA	10% of the cost quoted for development of the application phase as quoted in ***Annexure-VIII*** for the section "Financial Bid" in section “A” mentioned as - Total Cost for Development Phase	1
	4	User Training and its	10% of the cost quoted for development of the application phase as quoted in ***Annexure-VIII***	1

Section	Milestone Number	Payment Milestones	% Payment of Sub-total for Services Provided	Payment frequency for the year
		acceptance by PFRDA	for the section "Financial Bid" in section “A” mentioned as - Total Cost for Development Phase	
	5	Implementation/Go live and its acceptance by PFRDA	30% of the cost quoted for development of the application phase as quoted in ***Annexure-VIII*** for the section "Financial Bid" in section “A” mentioned as - Total Cost for Development Phase	1
(B) License Cost				
B.1	6	License Cost for Development Phase	This is required for the Development Phase. This cost will be paid in 3 parts. 50 % of the quoted cost in ***Annexure-VIII*** for the section "Financial Bid" in section “B.1” upon procurement, delivery, installation and submission of necessary documents of license in the name of PFRDA; 40% of the quoted cost in ***Annexure-VIII*** for the section "Financial Bid" in section “B.1” upon UAT signoff by PFRDA and 10% % of the quoted cost in ***Annexure-VIII*** for the section "Financial Bid" in section “B.1” upon Go Live signoff by PFRDA.	3
B.2	7	License/ Subscription Cost for Warranty & Stabilization Phase	100% of the cost quoted for one year of License /Subscription cost for warranty and Stabilization phase. This cost will be paid in advance. This should be as per the Bidder’s quote in ***Annexure-VIII*** under the section "Financial Bid", in subsection "B.2", labeled as " License /Subscription Cost for Warranty & Stabilization Phase."	1
B.3	8	License /Subscription Cost for 1st year AMC	100% of the cost quoted for one year of License /Subscription Cost for 1st year AMC. This cost will be paid in advance. This should be	1

Section	Milestone Number	Payment Milestones	% Payment of Sub-total for Services Provided	Payment frequency for the year
			as per the Bidder's quote in ***Annexure-VIII*** under the section "Financial Bid", in subsection "B.3", labeled as " License /Subscription Cost for 1st year AMC."	
B.4	9	License /Subscription Cost for 2nd year AMC	100% of the cost quoted for one year of License /Subscription Cost for 2nd year AMC. This cost will be paid in advance. This should be as per the Bidder's quote in ***Annexure-VIII*** under the section "Financial Bid", in subsection "B.4", labeled as " License /Subscription Cost for 2nd year AMC."	1
B.5	10	License /Subscription Cost for 3rd year AMC	100% of the cost quoted for one year of License /Subscription Cost for 3rd year AMC. This cost will be paid in advance. This should be as per the Bidder's quote in ***Annexure-VIII*** under the section "Financial Bid", in subsection "B.5", labeled as " License /Subscription Cost for 3rd year AMC."	1
B.6	11	License /Subscription Cost for 4th year AMC	100% of the cost quoted for one year of License /Subscription Cost for 4th year AMC. This cost will be paid in advance. This should be as per the Bidder's quote in ***Annexure-VIII*** under the section "Financial Bid", in subsection "B.6", labeled as " License /Subscription Cost for 4th year AMC."	1
(C) Warranty & stabilization phase				
C.1	12	Quarterly payment for Cloud	25% of the cost will be paid in each quarter for cloud cost. This is required for the warranty and development phase. This cost will be paid in quarterly basis after the	4

Section	Milestone Number	Payment Milestones	% Payment of Sub-total for Services Provided	Payment frequency for the year
			application goes live, upon submission of the necessary documents & invoices with SLA reports for PFRDA at the end of the quarter from the date of Go Live. This should be as per the Bidder's quote in ***Annexure-VIII*** under the section "Financial Bid", in subsection "B.2", labeled as "Cloud cost"	
C.2	13	Quarterly payment for Helpdesk	25% of the cost will be paid in each quarter for helpdesk. This is required for the warranty and development phase. This cost will be paid in quarterly basis after the application goes live, upon submission of the necessary documents & invoices with SLA reports for PFRDA at the end of the quarter from the date of Go Live. This should be as per the Bidder's quote in ***Annexure-VIII*** under the section "Financial Bid", in subsection "B.3", labeled as "Technical Helpdesk"	4
C.3	14	Quarterly payment for Facility Management	25% of the cost will be paid in each quarter for facility management at the end of the quarter. This is required for the warranty and development phase. This cost will be paid in end of quarter on quarterly basis after the application goes live, upon submission of the necessary documents & invoices with SLA reports for PFRDA at the end of the quarter from the date of Go Live. This should be as per the Bidder's quote in ***Annexure-VIII*** under the section "Financial Bid", in subsection "B.4", labeled as "Facility Management cost including manpower"	4

Section	Milestone Number	Payment Milestones	% Payment of Sub-total for Services Provided	Payment frequency for the year
C.4	15	Warranty & Stabilization cost for one year	25% of the cost will be paid in each quarter for Warranty & stabilization. This is required for the warranty and development phase. This cost will be paid in quarterly basis after the application goes live, upon submission of the necessary documents & invoices with SLA reports for PFRDA at the end of the quarter from the date of Go Live. This should be as per the Bidder's quote in ***Annexure-VIII*** under the section "Financial Bid", in subsection "B.5", labeled as "Warranty & Stabilization Cost".	4
C.5	16	Any other cost (mention item details in subsequent rows)	If the bidder quotes and uses any component not itemized in the Financial Bid but includes it in section B.6, it can be invoiced to PFRDA on a quarterly basis at 25%. This should align with the bidder's quote in ***Annexure-VIII***, under the "Financial Bid" section, in subsection "B.6", labeled as "Any other Cost."	4
(D) Total Cost for first year AMC				
D.1	17	Cloud Cost	25% of the cost will be paid in each quarter for cloud cost. This is required for the AMC phase. This cost will be paid in quarterly basis after the application goes in AMC phase, upon submission of the necessary documents & invoices with SLA reports for PFRDA at the end of the quarter. This should be as per the Bidder's quote in ***Annexure-VIII*** under the section "Financial Bid", in subsection "C.2", labeled as "Cloud cost"	4
D.2	18	Technical Helpdesk	25% of the cost will be paid in each quarter for helpdesk. This is required for the AMC phase. This	4

Section	Milestone Number	Payment Milestones	% Payment of Sub-total for Services Provided	Payment frequency for the year
			cost will be paid in quarterly basis, upon submission of the necessary documents & invoices with SLA reports for PFRDA at the end of the quarter. This should be as per the Bidder's quote in ***Annexure-VIII*** under the section "Financial Bid", in subsection "C.3", labeled as "Technical Helpdesk"	
D.3	19	AMC cost	25% of the cost will be paid in each quarter as AMC cost. This is required for the AMC phase. This cost will be paid in quarterly basis after the application goes in AMC phase, upon submission of the necessary documents & invoices with SLA reports for PFRDA at the end of the quarter. This should be as per the Bidder's quote in ***Annexure-VIII*** under the section "Financial Bid", in subsection "C.4", labeled as "AMC Cost".	4
D.4	20	Any other cost (mention item details in subsequent rows)	If the bidder quotes and uses any component not itemized in the Financial Bid but includes it in section C.5, it can be invoiced to PFRDA on a quarterly basis at 25%. This should align with the bidder's quote in ***Annexure-VIII***, under the "Financial Bid" section, in subsection "B.6", labeled as "Any other Cost."	4
(E) Total Cost for second year AMC				
E.1	21	Cloud Cost	25% of the cost will be paid in each quarter for cloud cost. This is required for the AMC phase. This cost will be paid in quarterly basis after the application goes in AMC phase, upon submission of the necessary documents & invoices with SLA reports for PFRDA at the end of the quarter. This should	4

Section	Milestone Number	Payment Milestones	% Payment of Sub-total for Services Provided	Payment frequency for the year
			be as per the Bidder's quote in ***Annexure-VIII*** under the section "Financial Bid", in subsection "D.2", labeled as "Cloud cost"	
E.2	22	Technical Helpdesk	25% of the cost will be paid in each quarter for helpdesk. This is required for the AMC phase. This cost will be paid in quarterly basis, upon submission of the necessary documents & invoices with SLA reports for PFRDA at the end of the quarter. This should be as per the Bidder's quote in ***Annexure-VIII*** under the section "Financial Bid", in subsection "D.3", labeled as "Technical Helpdesk"	4
E.3	23	AMC cost	25% of the cost will be paid in each quarter as AMC cost. This is required for the AMC phase. This cost will be paid in quarterly basis after the application goes in AMC phase, upon submission of the necessary documents & invoices with SLA reports for PFRDA at the end of the quarter. This should be as per the Bidder's quote in ***Annexure-VIII*** under the section "Financial Bid", in subsection "D.4", labeled as "AMC Cost".	4
E.4	24	Any other cost (mention item details in subsequent rows)	If the bidder quotes and uses any component not itemized in the Financial Bid but includes it in section D.5, it can be invoiced to PFRDA on a quarterly basis at 25%. This should align with the bidder's quote in ***Annexure-VIII***, under the "Financial Bid" section, in subsection "D.5", labeled as "Any other Cost."	4
(F) Total Cost for third year AMC				

Section	Milestone Number	Payment Milestones	% Payment of Sub-total for Services Provided	Payment frequency for the year
F.1	25	Cloud Cost	25% of the cost will be paid in each quarter for cloud cost. This is required for the AMC phase. This cost will be paid in quarterly basis after the application goes in AMC phase, upon submission of the necessary documents & invoices with SLA reports for PFRDA at the end of the quarter. This should be as per the Bidder's quote in ***Annexure-VIII*** under the section "Financial Bid", in subsection "E.2", labeled as "Cloud cost"	4
F.2	26	Technical Helpdesk	25% of the cost will be paid in each quarter for helpdesk. This is required for the AMC phase. This cost will be paid in quarterly basis, upon submission of the necessary documents & invoices with SLA reports for PFRDA at the end of the quarter. This should be as per the Bidder's quote in ***Annexure-VIII*** under the section "Financial Bid", in subsection "E.3", labeled as "Technical Helpdesk"	4
F.3	27	AMC cost	25% of the cost will be paid in each quarter as AMC cost. This is required for the AMC phase. This cost will be paid in quarterly basis after the application goes in AMC phase, upon submission of the necessary documents & invoices with SLA reports for PFRDA at the end of the quarter. This should be as per the Bidder's quote in ***Annexure-VIII*** under the section "Financial Bid", in subsection "E.4", labeled as "AMC Cost".	4
F.4	28	Any other cost (mention item details in	If the bidder quotes and uses any component not itemized in the Financial Bid but includes it in section E.5, it can be invoiced to	4

Section	Milestone Number	Payment Milestones	% Payment of Sub-total for Services Provided	Payment frequency for the year
		subsequent rows)	PFRDA on a quarterly basis at 25%. This should align with the bidder's quote in ***Annexure-VIII***, under the "Financial Bid" section, in subsection "E.5", labeled as "Any other Cost."	
(G) Total Cost for fourth year AMC				
G.1	29	Cloud Cost	25% of the cost will be paid in each quarter for cloud cost. This is required for the AMC phase. This cost will be paid in quarterly basis after the application goes in AMC phase, upon submission of the necessary documents & invoices with SLA reports for PFRDA at the end of the quarter. This should be as per the Bidder's quote in ***Annexure-VIII*** under the section "Financial Bid", in subsection "F.2", labeled as "Cloud cost"	4
G.2	30	Technical Helpdesk	25% of the cost will be paid in each quarter for helpdesk. This is required for the AMC phase. This cost will be paid in quarterly basis, upon submission of the necessary documents & invoices with SLA reports for PFRDA at the end of the quarter. This should be as per the Bidder's quote in ***Annexure-VIII*** under the section "Financial Bid", in subsection "F.3", labeled as "Technical Helpdesk"	4
G.3	31	AMC cost	25% of the cost will be paid in each quarter as AMC cost. This is required for the AMC phase. This cost will be paid in quarterly basis after the application goes in AMC phase, upon submission of the necessary documents & invoices with SLA reports for PFRDA at the end of the quarter. This should be as per the Bidder's quote in	4

Section	Milestone Number	Payment Milestones	% Payment of Sub-total for Services Provided	Payment frequency for the year
			Annexure-VIII under the section "Financial Bid", in subsection "F.4", labeled as "AMC Cost".	
G.4	32	Any other cost (mention item details in subsequent rows)	If the bidder quotes and uses any component not itemized in the Financial Bid but includes it in section F.5, it can be invoiced to PFRDA on a quarterly basis at 25%. This should align with the bidder's quote in ***Annexure-VIII***, under the "Financial Bid" section, in subsection "F.5", labeled as "Any other Cost."	4
H	33	500 man-days cost	Bidder should quote 500 man-days as a contingency for Change Requests (CR) over the project's tenure. In the Financial Bid but includes it in section H, it can be invoiced to PFRDA on an actual basis. This should align with the bidder's quote in ***Annexure-VIII***, under the "Financial Bid" section, in subsection "H", labeled as "500 man-days cost"	As per utilization during the project

Name & Signature of authorized signatory

Seal of Company

Annexure-X: Project Details and Client References

To whomsoever it may concern

Please fill details for each project:

Particulars	Details
Client Information	
Client Name	
Client address	
Name of the contact person and designation	
Phone number of the contact person	
e-mail address of the contact person	
Project Details	
Name of the Project	
Project Relevant Scope	
Project Technology Stack	
Use cases relevant to PFRDA requirements in brief	
Project duration (phase wise details, if any)	
Start Date	
End Date	
Current Status Completion Certificate from client (preferable), in case of project completed (Go Live)	
Whether AMC of the project's ownership is also with same SI	
Project hosted on	
Size of Project	
Value of Work Order (In Lakhs) (only single workorder)	
Location(s) where the project implemented	

Particulars	Details
No of Users	
Any other information	

Name & Signature of authorized signatory

Seal of Company

Annexure-XI: Certification By CSP

Sample format for CSP. Bid specific satisfactory MAF by CSP will also be accepted. It should mention that this would be valid for entire project duration.

[On the Letter head of CSP]

Date:

To,

Chief General Manager

In charge- PFRDA-TRACE

PENSION FUND REGULATORY AND DEVELOPMENT AUTHORITY(PFRDA)

B-14/A, Qutab Institutional Area, Chhatrapati Shivaji Bhavan, Katwaria Sarai, New Delhi-110016

Sub: Authorization letter from CSP to ----- (Bidder) for participation in bid for DESIGN, DEVELOPMENT, IMPLEMENTATION AND MAINTENANCE OF PFRDA-TRACE (PFRDA - TRACKING REPORTING ANALYTICS & COMPLIANCE e-PLATFORM)

Dear Sir,

Ref.: Authorization letter from CSP to ----- (Bidder) for participation in bid for RFP Reference No: PFRDA/2024/TARCH/PFRDA-TRACE/01

Particular	**Make & model/development/Unit details**
Cloud specifications and details	
<<Please insert details as required>>	
Other *(Please insert other Components, as required)*	

We hereby confirm our participation as CSP against this invitation for Bid by the above company/LLP.

We undertake to perform the requirements as set out in the RFP in respect of such services as mentioned in scope of work for CSP and hereby extend our services through

M/s.……during the …____ years contract period as per terms and conditions of the RFP.

We are MeitY empanelled CSP and also undertake that we have not been blacklisted by the Government Authority or Public Sector Undertaking (PSUs) in India or any Financial Institution in India as on date of submission of response.

Dated at _____ this _____ day of _____<YEAR>.

Yours faithfully,

Name & Signature of authorized signatory

Seal of Company

[Signature of Authorized Representative of CSP] [Title] [Organization stamp/seal] [Date]

Annexure-XII: Checklist of Documents to Be Submitted

S. No.	Documents to be submitted	Submitted (Y/N)	Documentary Proof (Page No.)
1.	Bid processing fee in the form of Account Payee Demand Draft. In case of online payment, receipt / acknowledgment of the bid processing fee.		
2.	Earnest Money Deposit (EMD) in the form of Performance Security. If the EMD is submitted in the form of Fixed Deposit or Online Payment – the Receipt of the same.		
3.	Integrity Pact (on Rs. One hundred (100) stamp paper)		
4.	Technical proposal as per the RFP requirements		
5.	Technical bid Covering Form as per ***Annexure-I***		
6.	Bidder details as per ***Annexure-II***		
7.	Financial Capability Statement as per ***Annexure-III***		
8.	Certificate of incorporation/ Copy of Certificate of Registration/LLP Registration		
9.	GST Registration Certificate		
10.	Power of attorney/board resolution to the authorized Signatory		
11.	Work order(s), completion certificates		
12.	Project details as per ***Annexure- X***		
13.	Valid CMMi level 3 Certificate or above		
14.	Valid ISO 9001, 27001 certificate from bidder		
15.	Valid MeitY empaneled certificate from Cloud Service Provider		
16.	Project Team structure with Resume of Key personnel as per ***Annexure - XVI***		

S. No.	Documents to be submitted	Submitted (Y/N)	Documentary Proof (Page No.)
17.	Audited financial statement for Financial years (i.e. FY 2022-23, FY 2021-22, FY 2020-21)		
18.	Certification (MAF) from OEM as per ***Annexure-VII***		
19.	Financial bid as per ***Annexure-VIII***		
20.	Project details and Client references as per ***Annexure-X***		
21.	Certification from CSP as per ***Annexure-XI***		
22.	Cloud Port Out Plan		
23.	Bidders undertaking on letter head for key manpower experience & qualification		

Name & Signature of authorized signatory

Seal of Company

Annexure-XIII: Completion Certificate

Date:

M/s. _____

Sub: Completion Certificate for design, development, and implementation of software solution

1. This is to certify that the Software Solution as detailed below has/have been successfully designed, developed, and implemented in accordance with the Contract/specifications.
    a. PO No. _____dated.
    _____
    b. Description of the Solution
    _____
    c. Date of installation
    _____
    d. Date of acceptance test
    _____
    e. Date of Go-live
    _____
    f. Project Completion date including warranty and AMC_____
2. The development and implementation have been done to our entire satisfaction and staff have been trained to operate the Software Solution.

Signature _____

Name_____

Designation with stamp _____

Annexure-XIV Change Request

PFRDA may consider utilising the services of bidder to implement additional Services that are not part of the scope of this RFP on time and material basis/man days rate basis. Bidders are requested to provide a man days rate option. It may be noted that PFRDA will invoke these rates for any further Change Requests once the efforts under man days as quoted in Man days bundle in this RFP have been exhausted. The man-days rate will be applicable for the entire project duration.

	Experience in years	**5 - 10**	**10+**
S. no.	**Development and operations**	**Monthly Rates in INR**	
1	Developers		
2	Mobile Application Developer		
3	UI/UX Designer		
4	Quality Assurance/Test Engineer		
5	Technical Document/Content Writer		
6	System and Database Operations Engineer		
7	Networking Operations Engineer		
8	Training and Change Management Engineer		
9	Information Security Engineer		
10	Data Science/Analytics Engineer		
11	Security Auditor		
12	Any similar nature of works comparable to the above		

Name & Signature of authorized signatory

Seal of Company

Annexure-XVI: Resume Format

Resume proposed for the role of – <<<<mention the proposed role of the candidate for this RFP>>>>

1. Name:
2. Designation:
3. Highest Qualification:
4. Relevant professional Certifications/Memberships:
5. Total Experience in years:
6. Relevant Experience in years:
7. Project details for relevant experience:
    a. Name of assignment or project:
    b. Duration (From – To):
    c. Location:
    d. Client Name:
    e. Scope of Work of project:
    f. Role:
    g. Activities performed:

A. Experience in proposed tools, technology, solution, methodology, nature of work, provide details:

Name & Signature of authorized signatory

Seal of Company

Annexure-XVII: Relevant Functional & Technical requirements

S. no.	Criteria	Yes/No	Client Name & Contact details (email & phone number)	Project Name & Relevant SoW	Project Duration (From - To)
1	The implemented solution should be able to send out automated emails alerts notifications, reports to all/defined stake holders.				
2	The implemented solution should have features of configuring roles, privileges & access management-based control.				
3	The implemented solution should use rule engine for detecting anomalies & raise flags as required by PFRDA.				
4	The implemented solution should be capable of integration with electronic and digital signature capabilities.				
5	The implemented solution should be able to integrate with systems of external organizations through APIs & other modes. The solution should be flexible so that any new user role could be on boarded in future.				
6	The implemented solution should be able to create basic workflows like adding new compliance reports, assign it to user groups, add relevant section in old reports or create new reports - by user department/PFRDA Admin.				
7	The implemented solution should be able to create web forms, assign them to user groups under category & subcategory - by user department/PFRDA Admin.				

Name & Signature of authorized signatory Seal of Company

Annexure-XVIII: Bill of Material for Licensed products & any other services used

All licensed products which are recommended in the architecture should be included in this table.

S. no	Product Name	Qty.	Vendor	License Type	Usage Notes

Name & Signature of authorized signatory

Seal of Company

Appendix I: Performance Bank Guarantee Format for EMD (Indicative)

To,

Chief General Manager

In charge- PFRDA-TRACE

Pension Fund Regulatory and Development Authority (PFRDA)

B-14/A, Qutab Institutional Area, Chhatrapati Shivaji Bhavan, Katwaria Sarai, New Delhi-110016

EMD Performance bank guarantee for Request for Proposal for SELECTION OF SYSTEM INTEGRATOR(SI) FOR DESIGN, DEVELOPMENT, IMPLEMENTATION AND MAINTENANCE OF PFRDA-TRACE (PFRDA - TRACKING REPORTING ANALYTICS & COMPLIANCE e-PLATFORM) which includes Regulatory/Supervisory/Analytics other ancillary modules for improving the efficiency and efficacy of these operations as are set out in the RFP NO.-_____ DATED _____

1. WHEREAS Pension Fund Regulatory and Development Authority (PFRDA), having its Office at Chhatrapati Shivaji Bhavan, Katwaria Sarai, B-14/A, Qutab Institutional Area Block B Rd, New Delhi-110016 has invited Request for Proposal to implement, customise, maintain and support the PFRDA-TRACE as are set out in the Request for Proposal RFP no. _____ dated _____.
2. It is one of the terms of said Request for Proposal that bidder shall furnish a Performance bank guarantee for a sum of Rs 1,20,00,000 (Rupees One Crore Twenty Lakhs only) as Earnest Money Deposit.
3. M/s._____, (hereinafter called as Bidder, who are our constituents intends to submit their Bid for the said work and have requested us to furnish guarantee in respect of the said of Rs 1,20,00,000 (Rupees One Crore Twenty Lakhs only)
4. Now this Guarantee witnesseth that

   We _____ (Bank) do hereby agree and undertake that in the event of PFRDA coming to the conclusion that bidder i.e. (Name of the entity) has not performed their obligations under the said conditions of the RFP or has committed a breach thereof, which conclusion shall be binding on us as well as the said Bidder, we shall on demand by PFRDA, pay to PFRDA, without demur or protest to PFRDA, a sum of Rs 1,20,00,000 (Rupees One Crore Twenty Lakhs only) . Our guarantee shall be treated as equivalent to the Earnest Money Deposit for the due performance of the obligations of bidder under the said conditions, provided, however, that our liability against such sum shall not exceed the sum of Rs 1,20,00,000 (Rupees One Crore Twenty Lakhs only)

5. We also undertake and confirm that the sum not exceeding Rs 1,20,00,000 (Rupees One Crore Twenty Lakhs only) as aforesaid shall be paid by us without any demur or protest, merely on demand from PFRDA on receipt of a notice in writing stating the amount is due to them and we shall not ask for any further proof or evidence and the notice from PFRDA shall be conclusive and binding on us and shall not be questioned by us in any respect or manner whatsoever. We undertake to pay the amount claimed by PFRDA, without protest or demur or without reference to Bidder and notwithstanding any contestation or existence of any dispute whatsoever between Bidder and PFRDA, pay PFRDA forthwith from the date of receipt of the notice as aforesaid. We confirm that our obligation to PFRDA under this guarantee shall be independent of the agreement or agreements or other understandings between PFRDA and bidder (Name). This guarantee shall not be revoked by us without prior consent in writing of PFRDA.
6. We hereby further agree that –
    a. Any forbearance or commission on the part of PFRDA in enforcing the conditions of the said agreement or in compliance with any of the terms and conditions stipulated in the said Bid and/or hereunder or granting of any time or showing of any indulgence by PFRDA to bidder or any other matter in connection therewith shall not discharge us in any way our obligation under this guarantee. This guarantee shall be discharged only by the performance of bidder of their obligations and in the event of their failure to do so, by payment by us of the sum not exceeding Rs 1,20,00,000 (Rupees One Crore Twenty Lakhs only).
    b. Our liability under these presents shall not exceed the sum of Rs 1,20,00,000 (Rupees One Crore Twenty Lakhs only).
    c. Our liability under this agreement shall not be affected by any infirmity or irregularity on the part of our said constituents in tendering for the said work or their obligations there under or by dissolution or change in the constitution of our said constituents.
    d. This guarantee shall remain in force for 180 days from the due date of closure of this RFP provided that if so desired by PFRDA, this guarantee shall be renewed for a further period as may be indicated by them on the same terms and conditions as contained herein.
    e. Our liability under these presents will terminate unless these presents are renewed as provided herein after completion of 180 days or on the day when our said constituents comply with their obligations, as to which a certificate in writing by PFRDA alone is the conclusive proof, whichever date is earlier.
    f. Unless demand for claim under this guarantee is made on us in writing on or before _____ (mention claim period with extension, if any), we shall be discharged from all liabilities under this guarantee thereafter.
    g. This guarantee shall be governed by Indian Laws and the Courts in Delhi, India alone shall have the jurisdiction to try & entertain any dispute arising out of this guarantee.

h. We, the Bank also agree that this guarantee will not be discharged due to change in the constitution of the Bank or _____(name of the purchasing entity).

Notwithstanding anything contained hereinabove:

1. Our liability under this guarantee shall not exceed Rs 1,20,00,000 (Rupees One Crore Twenty Lakhs only).
2. We shall not revoke the guarantee during its currency except with the previous consent of Pension Fund Regulatory and Development Authority in writing.
3. We are liable to pay the guaranteed amount or any part thereof under this bank guarantee only if you serve upon us a written claim or demand on or before the expiry of this guarantee.
4. ……

Yours faithfully, (For and on behalf of Authorised official of the bank)

(Note: This guarantee will require stamp duty and shall be signed by the official(s) whose signature and authority shall be verified)

Appendix-II: Performance Bank Guarantee Format for Performance Security (Indicative)

(TO BE STAMPED AS AN AGREEMENT)

Performance bank guarantee as performance security Selection of System Integrator (SI) For Design, Development, Implementation and Maintenance of PFRDA-Trace (PFRDA - Tracking Reporting Analytics & Compliance e-Platform) as are set out in the RFP NO.- _____ Dated _____

(Performa of Performance Bank Guarantee)

To,
Pension Fund Regulatory and Development Authority
B-14/A, Chhatrapati Shivaji Bhawan,
Qutab Institutional Area
Katwaria Sarai,
New Delhi-110016

Sub: Guarantee No. _____ for Rs. executed on this the_ day of _____ at _____ by ___*(Name of the Bank)* having its Head/Registered office at ____(hereinafter referred to as "the Guarantor" which expression shall unless it be repugnant to the subject or context thereof include successors and assigns).

In favour of Pension Fund Regulatory and Development Authority (hereinafter referred to as "PFRDA", which expression shall, unless repugnant to the context or meaning thereof include its administrators, successors or assigns.

Whereas

1. The Agreement ("AGREEMENT") dated……. being entered into between PFRDA and _____ ,
2. a company incorporated under the provisions of the Companies Act, 2013/ Limited liability Partnership firm registered under the Limited Liability Partnerships Act, 2008 having its registered office _____, Successful Bidder, for System Implementation at PFRDA (hereinafter referred to as "The Project").
3. As per terms of RFP, SI is required to furnish to PFRDA, an unconditional and irrevocable Performance Security for an amount of INR _____ only as security for due and punctual performance/discharge of its obligations under the Agreement relating to design, development and operate the system.

4. At the request of the Selected Bidder, the Guarantor has agreed to provide Performance Security, being these presents guaranteeing the due and punctual performance/discharge by SI of its obligations relating to the Project.

Now Therefore This Deed Witnesseth As Follows:

1. Capitalized terms used herein but not defined shall have the meaning assigned to them respectively in the Agreement.
2. The Guarantor hereby irrevocably guarantees the due and punctual performance by _____
3. (hereinafter called "the Selected Bidder") of all its obligations relating to the Project and in connection with design, development, and operation of software application/project by the Selected Bidder, in accordance with the Agreement.
4. The Guarantor shall, without demur or protest, pay to PFRDA sums not exceeding in aggregate INR_____, within ten (10) calendar days of receipt of a written demand therefor from PFRDA stating that the Company has failed to meet its obligations under the Agreement. The Guarantor shall not go into the veracity of any breach or failure on the part of SI or validity of demand so made by PFRDA and shall pay the amount specified in the demand, notwithstanding any direction to the contrary given or any dispute whatsoever raised by SI or any other Person. The Guarantor's obligations hereunder shall subsist until all such demands are duly met and discharged in accordance with the provisions hereof.
5. In order to give effect to this Guarantee, PFRDA shall be entitled to treat the Guarantor as the principal debtor. The obligations of the Guarantor shall not be affected by any variations in the terms and conditions of the Agreement or other documents or by the extension of time for performance granted to SI or postponement/non exercise/delayed exercise of any of its rights by PFRDA or any indulgence shown by PFRDA to SI and the Guarantor shall not be relieved from its obligations under this Guarantee on account of any such variation, extension, postponement, non-exercise, delayed exercise of any of its rights by PFRDA or any indulgence shown by PFRDA, provided nothing contained herein shall enlarge the Guarantor's obligation hereunder.
6. This Guarantee shall be irrevocable and shall remain in full force and effect until _____ (atleast180 days after completion of tenure of contract (including AMC)) unless discharged/released earlier by PFRDA in accordance with the provisions of the Agreement. The Guarantor's liability in aggregate be limited to a sum of INR.
7. This Guarantee shall not be affected by any change in the constitution or winding up of the Selected Bidder/the Guarantor or any absorption, merger, or amalgamation of the Concessionaire/the Guarantor with any other Person.
8. The Guarantor has power to issue this guarantee and discharge the obligations contemplated herein, and the undersigned is duly authorized to execute this Guarantee pursuant to the power granted under_____

9. This guarantee shall be governed by Indian Laws and the Courts in Delhi, India alone shall have the jurisdiction to try & entertain any dispute arising out of this guarantee.
10. No claim under this guarantee shall be entertained by us unless the same has been preferred by Pension Fund Regulatory and Development Authority (PFRDA) by the said date.
11. We hereby confirm that we have the power/s to issue this guarantee in your favour under the Constitution and business procedure of our Bank and the undersigned is/are the recipient of authority by express delegation of power/s and has/have full power/s to execute this Performance Bank Guarantee in your favour under the Power of Attorney issued by the Bank.
12. Notwithstanding anything contained hereinabove:
    a. Our liability under this guarantee shall not exceed Rs.----------
    b. We shall not revoke the guarantee during its currency except with the previous consent of Pension Fund Regulatory and Development Authority (PFRDA) in writing.
    c. We are liable to pay the guaranteed amount or any part thereof under this Bank Guarantee only if you serve upon us a written demand on or before the expiry of this guarantee.

All claims under the guarantee will be payable at New Delhi.

This guarantee will be returned to us as soon as the purpose for which it is issued is fulfilled.

Date_____

Place_____

Witness_____

(Bank’s common seal)

Appendix III- Integrity Pact

(To Be Stamped As An Agreement)

Pension Fund Regulatory and Development Authority is a statutory body, which operates within the legal framework of PFRDA Act, 2013, hereinafter referred to as "The Buyer", and……. hereinafter referred to as "Bidder/Contractor"

i. Preamble

The Buyer intends to award, under laid down organizational procedures, contract/s for ……. The Buyer values full compliance with all relevant laws of the land, rules, regulations, economic use of resources and of fairness/transparency in its relations with its Bidder(a) and/or Contractor(s).

For Pension Fund Regulatory and Development Authority, (PFRDA) Independent External Monitors (IEMs) are Shri Deepak Kashyap, IRTS (Retd.) and Shri Harishwar Dayal, IDSE (Retd.)

The contact details of the IEMs as per records, is as below: -

1. Shri Deepak Kashyap
   1162, ATS Tourmaline, Dwarka Expressway, Gurugram – 122017
   Email: - deepakkashyapnd02@gmail.com
2. Shri Harishwar Dayal
   H-2, Lawyers Colony, Bypass Road,
   Agra - 282 005 (UP)
   E-mail: dayalagra@gmail.com

ii. Commitments of the Buyer

The Buyer commits itself to take all measures necessary to prevent corruption and to observe the following principles:

1. No employee of the Buyer, personally or through family members, will in connection with the tender/RFP for, or the execution of a contract, demand, take a promise for or accept, for self or third person, any material or other benefits which the person is not legally entitled to.
2. The Buyer will, during the tender process treat all Bidder(s) with equity and reason. The Buyer will in particular, before and during the tender process, provide to all Bidder(s) the same information and will not provide to any Bidder(s) confidential/additional information through which bidder(s) could obtain an advantage in relation to the tender process or the contract execution.

3. The Buyer will exclude from the process all known prejudiced persons.
4. If the Buyer obtains information on the conduct of any of its employees which is a criminal offence under the IPC/PC Act, or if there be a substantive suspicion in this regard, the Buyer will inform the Chief Vigilance Office and in addition can initiate disciplinary actions.

iii. Commitments of bidder(s)/Contractor(s)

Bidder(s)/Contractor(s) commit themselves to take all measures necessary to prevent corruption. Bidder(s)/Contractor(s) commit themselves to observe the following principles during participation in the tender process and during the contract execution.

Bidder(s)/Contractor(s) will not, directly or through any other person or firm, offer, promise or give to any of the Buyer's employees involved in the tender process or the execution of the contract or to any third person any material or other benefit which he/she is not legally entitled to, in order to obtain in exchange any advantage of any kind whatsoever during the tender process or during the execution of the contract.

Bidder(s)/Contractor(s) will not enter with other Bidders into any undisclosed agreement or understanding, whether formal or informal. This applies in particular to prices, specifications, certifications, subsidiary contracts, submission or non-submission of bids or any other actions to restrict competitiveness or to introduce cartelization in the bidding process.

Bidder(s)/Contractor(s) will not commit any offence under the relevant IPC/PC Act; further bidder(s)/Contractor(s) will not use improperly, for purposes of competition or personal gain, or pass on to others, any information or document provided by the Buyer as part of the business relationship, regarding plans, technical proposals, and business details, including information contained or transmitted electronically.

Bidder(s)/Contractors(s) of foreign origin shall disclose the name and address of the Agents/representatives in India, if any. Similarly bidder(s)/Contractors(s) of Indian Nationality shall furnish the name and address of the foreign Buyers, if any. Further details as mentioned in the “Guidelines on Indian Agents of Foreign Suppliers” shall be disclosed by bidder(s)/Contractor(s). Further, as mentioned in the Guidelines all the payments made to the Indian agent/representative have to be in Indian Rupees only.

Bidder(s)/Contractor(s) will, when presenting their bid, disclose any and all payments made, is committed to, or intends to make to agents, brokers, or any other intermediaries in connection with the award of the contract.

Bidder(s)/Contractor(s) who have signed the Integrity Pact shall not approach the Courts while representing the matter to IEMs and shall wait for their decision in the matter.

(2) Bidder(s)/Contractor(s) will not instigate third persons to commit offences outlined above or be an accessory to such offences.

iv. Disqualification from tender process and exclusion from future contracts

If bidder(s)/Contractor(s), before award or during execution has committed a transgression through a violation of Clause 2, above or in any other form such as to put their reliability or credibility in question, the Buyer is entitled to disqualify bidder(s)/Contractor(s) from the tender process. The firm will be banned from all future business dealings also.

v. Compensation for Damages

If the Buyer has disqualified bidder(s) from the tender process prior to the award according to Clause 3, the Buyer is entitled to demand and recover the damages equivalent to Earnest Money Deposit/Bid Security.

If the Buyer has terminated the contract according to Clause 3, or if the Buyer is entitled to terminate the contract according to Clause 3, the Buyer shall be entitled to demand and recover from the Contractor compensation as provided under the contract besides damages.

vi. Previous transgression

Bidder declares that no previous transgressions occurred in the last three years with any other company in any country conforming to the anti-corruption approach or with any Central or State Government Organization, Central/State Government Autonomous bodies, Regulatory bodies, Public Sector Enterprise/Undertaking in India that could justify his exclusion from the tender process.

If bidder makes incorrect statement on this subject, he can be disqualified from the tender process.

vii. Equal treatment of all Bidders/Contractors

The Buyer will enter into agreements with identical conditions as this one with all Bidders and Contractors.

The Buyer will disqualify from the tender process all bidders who do not sign this Pact or violate its provisions.

viii. Criminal charges against violating Bidder(s)/Contractor(s)

If the Buyer obtains knowledge of conduct of a Bidder, Contractor, or Subcontractor, or of an employee or a representative or an associate of a Bidder, Contractor or Subcontractor which constitutes corruption, or if the Buyer has substantive suspicion in this regard, the Buyer will inform the same to the Chief Vigilance Officer.

ix. **Independent External Monitor**

The Buyer appoints competent and credible Independent External Monitor for this Pact after approval by Central Vigilance Commission. The task of the Monitor is to review independently and objectively, whether and to what extent the parties comply with the obligations under this agreement.

The Monitor is not subject to instructions by the representatives of the parties and performs his/her functions neutrally and independently. The Monitor would have access to all contract documents, whenever required. It will be obligatory for him/her to treat the information and documents of bidders/Contractors as confidential. He/she reports to the Chairperson, PFRDA.

Bidder(s)/Contractor(s) accepts that the Monitor has the right to access without restriction to all project documentation of the Buyer including that provided by the Contractor. The contractor will also grant the Monitor, upon his/her request and demonstration of a valid interest, unrestricted and unconditional access to their project documentation.

The Monitor is under contractual obligation to treat the information and documents of bidder(s)/Contractor(s) with confidentiality. 'In case of any conflict of interest arising at a later date, the IEM shall inform Chairperson, PFRDA and recuse himself/herself from that case.

The Buyer will provide to the Monitor sufficient information about all meetings among the parties related to the Project provided such meetings could have an impact on the contractual relations between the Buyer and the Contractor. The parties offer to the Monitor the option to participate in such meetings.

As soon as the Monitor notices, or believes to notice, a violation of this agreement, he/she will so inform the Management of the Buyer and request the Management to discontinue or take corrective action, or to take other relevant action. The monitor can in this regard submit non-binding recommendations. Beyond this, the Monitor has no right to demand from the parties that they act in a specific manner, refrain from action, or tolerate action.

The Monitor will submit a written report to the Chairperson, PFRDA within 8 to 10 weeks from the date of reference or intimation to him by the Buyer and, should the occasion arise, submit proposals for correcting problematic situations.

If the Monitor has reported to the Chairperson, PFRDA, a substantiated suspicion of an offence under relevant IPC/PC Act, and the Chairperson, PFRDA has not, within the reasonable time taken visible action to proceed against such offence or reported it to the Chief Vigilance Officer, the Monitor may also transmit this information directly to the Central Vigilance Commissioner.

The work **'Monitor'** would include both singular and plural.

x. Pact Duration

This pact begins when both parties have legally signed it. It expires for the Contractor 180 days after the last payment under the contract, and for all other Bidders 180 days after the contract has been awarded to the successful bidder. Any violation of the same would entail disqualification of bidders and exclusion from future business dealings. If any claim is made/lodged during this time, the same shall be binding and continue to be valid despite the lapse of this pact as specified above, unless it is discharged/determined by Chairperson of PFRDA.

xi. Other Provisions

This agreement is subject to Indian Law. Place of performance and jurisdiction is the Registered Office of the Buyer, i.e. Delhi.

1. Changes and supplements as well as termination notices need to be made in writing. Side agreements have not been made.
2. Should one or several provisions of this agreement turn out to be invalid, the remainder of this agreement remains valid. In this case, the parties will strive to come to an agreement to their original intentions.
3. Issues like Warranty/Guarantee etc. shall be outside the purview of IEMs.
4. Bidder(s) shall not approach the courts while representing the matters to IEMs and he/she will await their decision in the manner.

Buyer	**Bidder**
Name of Officer	Chief Executive Officer/ Authorized Representative of Bidder
Designation	
PFRDA	

WITNESS	**WITNESS**
1.	1.
2.	2.

Appendix IV -Indicative Service Level Agreement (SLA) and Liquidated Damages

Service Level Agreement (SLAs) defines the quality and timelines of service delivery of a project. SLA helps PFRDA to sustain the planned business outcomes from the solution deployed on a continued basis over a sustained period of time.

i. Purpose of this Agreement

The purpose of this SLA is to clearly define the service level standards in terms of quality and timelines to be provided by SI and further enforce it on SI. SLA in this project shall be in effect for the entire contract period.

The SLA is designed to:

1. Define unambiguously the service level standards expected from SI and also ensure that the desired/agreed level of services rendered by SI to PFRDA.
2. Motivate SI to ensure the service standards are up to the mark.
3. Draw the urgent attention of SI in case there is any issues in the service levels or service level falls below the agreed/desired level.
4. Provide a tool to PFRDA to control and ensure the service levels provided by SI.
5. Avoid imposing compensation on SI without valid reason.

ii. Escalation Mechanism

The SLA provides the Levels of support to be provided by SI along with other important information like criticality of reported incident, incident escalations, responsible office(s) and expected time to resolve the incident. The following characteristics are used to identify the severity of an incident.

1. Service Category
2. Service Availability
3. Performance Metrics
4. Support and Escalation
5. Security and Data Protection
6. System Maintenance and Updates
7. Disaster Recovery and Business Continuity
8. Reporting and Communication

Table 1: Escalation Matrix

Escalation level	Severity Codes	Responsible Officer
Level 1	Critical High Medium Low	SI's service desk executive/Single point of Contact (SPOC) for software solution
Level 2	Critical High Medium Low	SI's Project Manager of software solution
Level 3	Critical High Medium Low	SI's Project Director of software solution

1. Availability of IT system - High Availability is a key requirement of PFRDA. The expected availability of IT system should not be less than 99.5%. The project must also be able to rebound or recover from any planned or unplanned system downtime, ensuring a minimal impact on the operations. SI should provide a single point of contact on a 24×7 basis.
2. Availability will be measured on quarterly basis. Planned downtime will not be classified as unavailability. Planned downtime where both main as well redundant systems are not available for providing service will be limited to maximum of 48 Hours in a quarter. SI should endeavour to take such downtimes only during weekends or holidays preferably after end of day (EoD). However, duration of the maximum allowable planned downtime time will be reviewed on half yearly/yearly basis.

iii. Service Windows & Severity Levels

Table 2: Application Module/Functionality wise Severity Matrix

1. **Severity Level 1 (Critical)**
    a. Impact: Severe disruption to core functionality, regulatory reporting.
    b. Urgency: Immediate action required, with potential legal or financial consequences.
    c. Actions: Immediate resolution and escalation to appropriate authorities. Continuous updates and communication until resolved.
2. **Severity Level 2 (High)**
    a. Impact: Significant disruption to regulatory reporting or critical processes.

b. Urgency: Urgent action required, with potential operational and regulatory impact.
c. Actions: Expedited resolution, escalation as needed, and regular updates to stakeholders.

3. **Severity Level 3 (Medium)**
   a. Impact: Moderate disruption to non-critical processes or functionality.
   b. Urgency: Action required within the regular operational timeframe.
   c. Actions: Resolution as part of regular operational procedures, with updates to affected parties.
4. **Severity Level 4 (Low)**
   a. Impact: Minor issues or non-critical requests.
   b. Urgency: Action required within a reasonable timeframe.
   c. Actions: Resolution as part of routine maintenance or next available support window.

iv. Service Levels

Following service levels will be applicable on SI during the entire maintenance period:

Table 3: Service Levels

Sr. No	Severity Level as per Application Module/ Functionality	Response Time/Acknowledgement of Problem	Resolution Time
1.	Critical	Within thirty (30) mins of reporting	Within two (02) hrs. of acknowledgement
2.	High	Within one (01) hr of reporting	Within six (06) hrs. of acknowledgement
3.	Medium	Within one (01) hr of reporting	Within twenty-Four (24) hrs. of acknowledgement
4.	Low	Within one (01) hr of reporting	Within Forty-Eight (48) hrs. of acknowledgement

v. In case of Failure to meet Service Levels

Following compensation shall be payable by SI in case of non-compliance to service levels (as provided in table above):

Table 4: Indicative Compensation in case of Non-compliance

Contract Price = TCO

Service Category	Service Level Agreement	Breach Threshold	Liquidated Damages
Service Availability	Service Availability: This measures the expected uptime and availability of PFRDA-TRACE	System availability falling below 99.5% in a calendar month	1% of monthly contract price of AMC phase per hour of system unavailability breaching the threshold
Performance Metrics	System Response Time: This measures the target response time for key operations such as record addition, retrieval, search, and upload.	Exceeding 10 seconds for average response time to user requests. This SLA will be measured randomly in a month in presence of the representative of SI.	5% of monthly contract price of AMC phase per incident of response time exceeding the threshold
Support and Escalation	Resolution Time: This measures the timeframe within which SI resolves the requests or issues.	- Severity 4 Issue Resolution Time >= 48 hours from the time the complaint/query is allocated for resolution by SI.	- INR 2,000 per ticket per day for delay of every additional day
		- Severity 3 Issue Resolution Time >= 24 hours from the time the complaint/query is allocated for resolution by SI.	- INR 2,500 per ticket per day for delay of every additional day
		- Severity 2 Issue Resolution Time >= 06 Hours from the time the complaint/query is allocated for resolution by SI.	- INR 5,000 per ticket per hour delay in resolution time.

Service Category	Service Level Agreement	Breach Threshold	Liquidated Damages
		- Severity 1 Issue Resolution Time =< T (T=02 hours maximum value) from the time the complaint/query is allocated for resolution by the Helpdesk. Time <= T (As agreed upon by PFRDA and SI) from the time the complaint/query is allocated for resolution by SI.	- INR 10,000 per ticket per hour delay in resolution time
Security and Data Protection:	Data Security Measures: Describes resolution time to any security incidents	- Exceeding 24 hours for resolution time to security incidents	- 10% of monthly contract price for each security vulnerability discovered and not remediated within timeframe communicated by PFRDA.
	Data Backup and Recovery: This measures instances of failure to perform scheduled backups or inability to recover data	- Failure to perform scheduled backups or inability to recover data	- 5% of monthly contract price per missed backup
	Conducting Security Audit every 1 year by CERT-In empaneled agency and Compliance	- First Security Audit to be done within 1 month from UAT Acceptance and thereafter every 1 year	- 2% of monthly contract price per week of delay in conducting Security Audit and Compliance
System Maintenance and Updates:	Maintenance Updates: This verifies that one version earlier than the latest patches	- Non update of security patches of Operating System, Database and Other Software	- 2% of monthly contract price per week of delay in applying updates

Service Category	Service Level Agreement	Breach Threshold	Liquidated Damages
	released by Original Manufacturer of software are applied by SI	components up to 1 level less than those released by Original Manufacturers of such software on quarterly basis	
Disaster Recovery and Business Continuity:	Recovery time objectives (RTO) and recovery point objectives (RPO).	- RTO > 2 hours or RPO > 30 minutes	- 5% of monthly contract price per hour of downtime exceeding RTO and 5% of monthly contract price for data loss exceeding RPO or 10% if breach of both RTO and RPO is applicable.
	Conducting Mock Drill every 6 months	- Delay in conducting mock drill for more than 1 week	- 2% of monthly contract price per week of delay in conducting Mock Drill
Reporting and Communication:	Performance Reports: This measures the frequency of submission of performance reports to be provided by SI, including system availability, response times, and support statistics.	- Non submission of reports on all SLAs listed in this section for every month on or before 10th of next month	- 2% of monthly contract price per missed report

vi. SLA Supervision

1. Performance Reporting Procedures: SI shall prepare the SLA performance reports of each quarter in an agreed upon format by the 10th calendar day of subsequent quarter. The reports will include details of each and every incident reported to SI i.e. date and time of receiving email/call, date and time of response/acknowledgement email, date and time of resolution provided for the reported problem, name of the module/functionality which is not working up to the mark, severity level of the module/functionality, complied to the service level or not, total number of incidents

reported, total number and % of non-compliance to the service level etc. Performance reports along with all the documentary proofs i.e. printouts of all the incident reporting emails/photocopies of incident log register, acknowledgement email, resolution email, resolution confirmation emails etc. and will be submitted to PFRDA in hardcopy as well as softcopy format (pdf, MS-Excel, or open office format). However actual performance reporting mechanism, format and list of supporting documents will be discussed and finalized by SI with PFRDA before entering into project maintenance phase.

2. PFRDA will be responsible for monitoring the performance of SI against the SLA parameters each quarter, or at any periodicity defined in the contract document/mutually decided by both the parties. The review/audit report prepared based on the performance report, will form basis for any action relating to compensation or breach of contract. Any such review/audit can be scheduled as and when required. The results will be shared with SI as soon as possible. PFRDA reserves the right to ask SI to provide performance report anytime during the contract period and to appoint a third-party auditor to validate the SLA.

vii. SLA Change Control

1. Any request for change in the service levels provided during the term of this agreement shall be documented and negotiated in good faith by both parties. Either party can request for a change. Changes will be documented as an addendum to SLA and consequently the contract.
2. If in cases there is any conflict between RFP document and the Contract, the Contract, and subsequent amendments, if any, shall prevail.

viii. Version Control

All negotiated SLA changes will require changing the version control number. As appropriate, minor changes may be accumulated for periodic release (e.g. every quarter) or for release when a critical threshold of change has occurred.

ix. Issue Management Process

This process provides an appropriate management structure for the orderly consideration and resolution of business and operational issues in the event that quick consensus is not reached between PFRDA and SI. It is expected that this pre-defined process will only be used on an exception basis if issues are not resolved at lower management levels.

1. Either PFRDA or SI may raise an issue by documenting the business or technical problem, which presents a reasonably objective summary of both points of view and identifies specific points of disagreement with possible solutions.
2. A meeting or conference call may be conducted to resolve the issue in a timely manner.

3. In the event, if the issue is still unresolved, PFRDA will decide on the matter as it deemed fit.

x. Issue Escalation Process

1. All issues would be raised to the designated representative of SI, who is completely responsible for the day-to-day aspects of the issue resolution.
2. If the representative of SI is unable to resolve an issue, the issue would be escalated to the next level as per escalation matrix.
3. In the event, if the issue is still unresolved, PFRDA will decide on the matter as it deemed fit.

xi. Risk and Cost Factor

In the event of termination of contract on the basis of non-performance by SI, SI will be solely responsible for risk and cost factor thereon. In such an event, the performance Security furnished by SI will be encashed and will stand forfeited.

xii. Cloud SLA Reports by SI

Deliverables listed below should be accessible via online interface not later than 10 days after the end of the calendar month and available for up to one year after creation. The information shall be available in format approved by MeitY. CSP shall monitor and maintain the stated service levels as agreed in the Service Level Agreement between PFRDA and SI. SI/CSP should configure their tool to track and monitor the SLA and the same system generated SLA reports at monthly basis.

SI shall workout the formats for the MIS reports and get these approved by PFRDA.

Service Level Management: Service Level Management reports to be available in the dashboard on real-time basis as mentioned below:

1. Service Availability at the VM & Service Availability at the Storage Level (Measured as Total Uptime Hours/Total Hours within the Month) displayed as a percentage of availability up to one-tenth of a percent (e.g. 99.5%)
2. Text description of major outages (including description of root-cause and fix) resulting in greater than 1-hour of unscheduled downtime within a month
3. The following details would be available in CSP dashboard for PFRDA. PFRDA may access these reports at any point of time.

xiii. Compensation for delayed implementation

The Authority expects that the successful bidder completes the scope of work within the timeframe. Inability of the successful bidder to either provide the requirements as per the scope

or to meet the timelines as specified would be treated as breach of contract and would invoke this clause. In case of the Go-Live delays by the Bidder the compensation as per PFRDAs discretion will be imposed on the Bidder 5% of the total contract value per month of delay, to the maximum of 10% of the total contract value as per the agreement between PFRDA and the successful Bidder.

Thereafter, at the discretion of the Authority, the contract may be cancelled (if this more than 1 quarter). The Authority may also invoke the Performance Guarantee, seek compensation on delay which is not attributable to Authority and is attributable to the successful Bidder.

The bidder should ensure implementation of the software application with all the functional, technical and security requirements as specified in the RFP document.

Notwithstanding anything contained above, no such compensation will be chargeable on the selected bidder for the inability occasioned, if such inability is due to reasons entirely attributable to Authority.

xiv. Breach of SLA

In case SI does not meet the service levels mentioned in this RFP and percent of non-compliance reaches 50%, PFRDA will treat it as a case of breach of Service Level Agreement. The following steps will be taken in such a case:

1. PFRDA issues a show cause notice to SI.
2. SI should reply to the notice within five working days.
3. If PFRDA is not satisfied with the reply, PFRDA will initiate termination process as per the contract.

xv. Limitation of Liability

System Integrator shall be excused and not be liable or responsible for any delay or failure to perform the Services or failure of the Services or a Deliverable to the extent that such delay or failure has arisen as a result of any delay or failure by PFRDA or third-party SIs to perform any of its duties and obligations as set out in this Agreement. In the event that SI is delayed or prevented from performing its obligations due to such failure or delay on the part of or on behalf of PFRDA, then the Solution Provider shall be allowed an additional period of time to perform its obligations and unless otherwise agreed the additional period shall be equal to the amount of time for which SI is delayed or prevented from performing its obligations due to such failure or delay on the part of or on behalf of PFRDA. Such failures or delays shall be brought to the notice of PFRDA, immediately within two (02) days of occurrence such failures or delays and subject to mutual agreement with PFRDA, the Solution Provider shall take such actions as may be necessary to correct or remedy the failures or delays and maintain record of all such incidents.

Notwithstanding anything contained in this Agreement the total cumulative liability of either party arising from or relating to this Contract shall not exceed 10% of TCO by PFRDA under this Agreement (excluding the taxes, reimbursements etc.), however, that this limitation shall not apply to any liability for damages arising from (a) wilful misconduct or (b) indemnification against third party claims for infringement.

Neither party shall be liable to the other for any indirect , incidental, consequential , exemplary, or punitive damages, loss of profits of revenue , loss of business whether in contract , TORT, or other theories of law. Even if such party have been advised of the possibility of such damages.

xvi. Exclusions

SI will be exempted from any non-compliance/delays/slippages on SLA parameters arising out of following reasons:

1. Delay in execution due to delay (in approval, review etc.) from PFRDA's side. Any such delays will be notified in written to PFRDA.
2. Force Majeure
3. Any other issues which are beyond the control of SI. Such issues to be notified to PFRDA.
4. PFRDA will have the right to decide as to whether SI is justified in raising such issues.

xvii. Other Conditions

Compensation payable by successful bidder will be recovered from the bills. No payment due will be released/adjusted before penalty due is paid by vendor.

There would be no payment for man-days invested in removing defects in developments.

In case of non-replacement of resource within two weeks after the release of existing resource, a compensation of Rs. 10,000/- per day will be payable till the new and suitable resource is provided. The waiver can only be permitted by Authority in befitting situations as per discretion of the Authority.

The compensation is payable at the rate of 10% of the annual payment for each instance of violation if the bidder fails to protect data breach.

The maximum compensation on account of all above instances will be 10% of the total cost of the project.

Appendix V: Draft Non-Disclosure and Confidentiality Agreement (Indicative)

This Reciprocal Non-Disclosure Agreement (the "Agreement") is. made at_____

_____

between:

Pension Fund Regulatory and Development Authority (PFRDA) having its office at Chhatrapati Shivaji Bhavan, , B-14/A, Qutab Institutional Area Katwaria Sarai, New Delhi-110016 ((hereinafter referred to as "Authority" which expression includes its successors and assigns) of the One Part.

And

A private/public limited company/LLP/Firm *<strike off whichever is not applicable>* incorporated under the provisions of the Companies Act, 1956/2013/Limited Liability Partnership Act 2008 *<strike off whichever is not applicable>*, having.

its registered office at_____(hereinafter referred to as

"_____" which expression shall unless repugnant to the subject or context thereof, shall mean and include its successors and permitted assigns) of the OTHER PART.

And Whereas

_____is carrying on business of providing_____, has agreed to

_____for PFRDA and other related tasks.

Each of the parties mentioned above are collectively referred to as the 'Parties' and individually as a 'Party'.

For purposes of advancing their business relationship, the parties would need to disclose certain valuable confidential information to each other (the Party receiving the information being referred to as the "Receiving Party" and the Party disclosing the information being referred to as the "Disclosing Party. Therefore, in consideration of covenants and agreements contained herein for the mutual disclosure of confidential information to each other, and intending to be legally bound, the parties agree to the terms and conditions as set out hereunder.

Now It Is Hereby Agreed By and Between The Parties As Under

i. Confidential Information and Confidential Materials

1. "Confidential Information" means non-public information that Disclosing Party designates as being confidential or which, under the circumstances surrounding disclosure ought to be treated as confidential. "Confidential Information" includes,

without limitation, information relating to developed, installed or purchased Disclosing Party software or services products, the information relating to general architecture of Disclosing Party's network, information relating to nature and content of data stored within network or in any other storage media, Disclosing Party's business policies, practices, methodology, policy design delivery, and information received from others that Disclosing Party is obligated to treat as confidential. Confidential Information disclosed to Receiving Party by any Disclosing Party Subsidiary and/or agents is covered by this agreement.

2. Confidential Information shall not include any information that: (i) is or subsequently becomes publicly available without Receiving Party's breach of any obligation owed to Disclosing party; (ii) becomes known to Receiving Party free from any confidentiality obligations prior to Disclosing Party's disclosure of such information to Receiving Party; (iii) became known to Receiving Party from a source other than Disclosing Party other than by the breach of an obligation of confidentiality owed to Disclosing Party and without confidentiality restrictions on use and disclosure; or (iv) is independently developed by Receiving Party.
3. "Confidential Materials" shall mean all tangible materials containing Confidential Information, including without limitation written or printed documents and computer disks or tapes, whether machine or user readable.

ii. Restrictions and obligations

1. Each party shall treat as confidential the Contract and any and all information ("confidential information") obtained from the other party pursuant to the Contract and shall not divulge such information to any person (except to such party's "Covered Person" which term shall mean employees, contingent workers and professional advisers of a party who need to know the same) without the other party's written consent provided that this clause shall not extend to information which was rightfully in the possession of such party prior to the commencement of the negotiations leading to the Contract, which is already public knowledge or becomes so at a future date (otherwise than as a result of a breach of this clause). Receiving Party will have executed or shall execute appropriate written agreements with Covered Person, sufficient to enable it to comply with all the provisions of this Agreement. Any breach of this Agreement by Receiving Party's Covered Person or Sub-Contractor shall also be constructed a breach of this Agreement by Receiving Party.
2. Receiving Party may disclose Confidential Information in accordance with judicial or other governmental order to the intended recipients (as detailed in this clause), provided Receiving Party shall give Disclosing Party reasonable notice (provided not restricted by applicable laws) prior to such disclosure and shall comply with any applicable protective order or equivalent. The intended recipients for this purpose are:
    a. the statutory auditors of the either party and government or regulatory authorities regulating the affairs of the parties and inspectors and supervisory bodies thereof.

b. Confidential Information and Confidential Material may be disclosed, reproduced, summarized, or distributed only in pursuance of Receiving Party's business relationship with Disclosing Party, and only as otherwise provided hereunder. Receiving Party agrees to segregate all such Confidential Material from the confidential material of others in order to prevent mixing.

iii. Rights and Remedies

1. Receiving Party shall notify Disclosing Party immediately upon discovery of any unauthorized used or disclosure of Confidential Information and/or Confidential Materials, or any other breach of this Agreement by Receiving Party and will cooperate with Disclosing Party in every reasonable way to help Disclosing Party regain possession of the Confidential Information and/or Confidential Materials and prevent its further unauthorized use.
2. Receiving Party shall return all originals, copies, reproductions and summaries of Confidential Information or Confidential Materials at Disclosing Party's request, or at Disclosing Party's option, certify destruction of the same.
3. Receiving Party acknowledges that monetary compensation may not be the only and/or a sufficient remedy for unauthorized disclosure of Confidential Information and that disclosing party shall be entitled, without waiving any other rights or remedies (including but not limited to as listed below), to injunctive or equitable relief as may be deemed proper by a Court of competent jurisdiction.
    a. Suspension of access privileges
    b. Change of personnel assigned to the job Termination of contract.
    c. Disclosing Party may visit Receiving Party's premises, with reasonable prior notice and during normal business hours, to review Receiving Party's compliance with the term of this Agreement.

iv. Miscellaneous

1. All Confidential Information and Confidential Materials are and shall remain the sole property of Disclosing Party. By disclosing information to Receiving Party, Disclosing Party does not grant any expressed or implied right to Receiving Party to disclose information under the Disclosing Party's patents, copyrights, trademarks, or trade secret information.
2. Confidential Information made available is provided "As Is," and disclosing party disclaims all representations, conditions, and warranties, express or implied, including, without limitation, representations, conditions or warranties of accuracy, completeness, performance, fitness for a particular purpose, satisfactory quality and merchantability provided same shall not be construed to include fraud or wilful default of disclosing party.

3. Neither party grants to the other party any license, by implication or otherwise, to use the Confidential Information, other than for the limited purpose of evaluating or advancing a business relationship between the parties, or any license rights whatsoever in any patent, copyright or other intellectual property rights pertaining to the Confidential Information.
4. The terms of Confidentiality under this Agreement shall not be construed to limit either party's right to independently develop or acquire product without use of the other party's Confidential Information. Further, either party shall be free to use for any purpose the residuals resulting from access to or work with such Confidential Information, provided that such party shall maintain the confidentiality of the Confidential Information as provided herein. The term "residuals" means information in non-tangible form, which may be retained by person who has had access to the Confidential Information, including ideas, concepts, know-how or techniques contained therein. Neither party shall have any obligation to limit or restrict the assignment of such persons or to pay royalties for any work resulting from the use of residuals. However, the foregoing shall not be deemed to grant to either party a license under the other party's copyrights or patents.
5. This Agreement constitutes the entire agreement between the parties with respect to the subject matter hereof. It shall not be modified except by a written agreement dated subsequently to the date of this Agreement and signed by both parties. None of the provisions of this Agreement shall be deemed to have been waived by any act or acquiescence on the part of Disclosing Party, its agents, or employees, except by an instrument in writing signed by an authorized officer of Disclosing Party. No waiver of any provision of this Agreement shall constitute a waiver of any other provision(s) or of the same provision on another occasion.
6. In case of any dispute, the same shall be decided in accordance with the arbitration clause governing the parties in the master agreement.
7. Subject to the limitations set forth in this Agreement, this Agreement will inure to the benefit of and be binding upon the parties, their successors, and assigns. This agreement at all times shall be subject to terms of RFP and the master service agreement, which shall prevail.
8. If any provision of this Agreement shall be held by a court of competent jurisdiction to be illegal, invalid, or unenforceable, the remaining provisions shall remain in full force and effect.
9. This Agreement may be amended only by a document in writing executed by a duly authorized official of each Party hereto, which shall form a part of the present Agreement.
10. The validity and interpretation of this Agreement and the legal relations of the parties to it shall be governed by the laws of India and shall be subject to the exclusive jurisdiction of the Courts in New Delhi.
11. The Agreement shall be effective from

("Effective Date") and shall be valid for a period of 180 days from the contract

completion date. The foregoing obligations as to confidentiality shall survive the term of this Agreement and thereafter provided confidentiality obligations with respect to individually identifiable information, customer's data of Parties or software in human-readable form (e.g., source code) shall survive in perpetuity.

v. Suggestions and Feedback

Either party from time to time may provide suggestions, comments, or other feedback to the other party with respect to Confidential Information provided originally by the other party (hereinafter "feedback"). Both parties agree that all Feedback is and shall be entirely voluntary and shall not in absence of separate agreement, create any confidentially obligation for the receiving party. However, the Receiving Party shall not disclose the source of any feedback without the providing party's consent. Feedback shall be clearly designated as such and, except as otherwise provided herein, each party shall be free to disclose and use such Feedback as it sees fit, entirely without obligation of any kind to other party. The foregoing shall not, however, affect either party's obligations hereunder with respect to Confidential Information of other party.

Dated this____day of_(Month) *2024* at_____(place)

For and on behalf of _

Name	_____	_____
Designation	_____	_____
Place	_____	_____
Signature	_____	_____

For and on behalf of _

Name	_____	_____
Designation	_____	_____
Place	_____	_____
Signature	_____	_____

Appendix VI: Draft Master Service Agreement (Indicative)

This Master Service Agreement ("Agreement") is made on this the <<Date>> day of <<Month>> <<Year>> at <<Place>>, India.

BETWEEN

Pension Fund Regulatory and Development Authority through **<<Name of the Officer>> <<Designation>>, PFRDA** having its office at B-14/A, Chatrapati Shivaji Bhawan, Qutub Institutional Area, Katwaria Sarai New Delhi-110016 , India hereinafter referred to as **'PFRDA' or 'Authority',** which expression shall, unless the context otherwise requires, include its permitted successors, and assigns).

AND

<<Company Name>>**,** company registered under the provisions of the Indian Companies Act, 1956/2013 or a firm registered under the Limited Liability Partnerships Act, 2008, having its registered office at <<Company Address>> (hereinafter referred to as '***System Integrator/SI'*** which expression shall, unless the context otherwise requires, include its permitted successors and assigns).

Each of the parties mentioned above are collectively referred to as

the '***Parties***' and individually as a '***Party***'.

WHEREAS:

PFRDA is desirous to implement the project for "Selection of System Integrator(SI) for Design, Development, Implementation and Maintenance of PFRDA-TRACE (PFRDA - Tracking Reporting Analytics & Compliance e-Platform) which is a very significant project for performance of its roles, duties and functions and will be a comprehensive, structured, and seamlessly integrated software solution for managing and automating a comprehensive data management system that encompasses data retrieval, storage, validation and the execution of various data analytics procedures. Additionally, the project aims to streamline and automate external stakeholder/intermediaries' interactions in accordance with the existing provisions of PFRDA Act, Rules, and Regulations.

This initiative anticipates a substantial reduction in manual processes, including document handling, data entry, processing, and long-term data storage, by the implementation of an integrated software solution. The envisioned solution is expected to facilitate efficient data processing, analysis, reporting, retrieval, management, and reorganization through automated workflows.

In furtherance of the same, PFRDA undertook the selection of a suitable System Integrator through an open competitive Bidding process for implementing the Project and in this behalf issued Request for Proposal (RFP) dated 31st January 2024 on PFRDA website www.pfrda.org.in under Tenders Section and https://eprocure.gov.in/epublish/app on 31st January 2024 with the last date of submission was ---date---> and Addendum/Corrigendum to the Request for Proposal (if any).

The successful bidder has been selected as the System Integrator on the basis of the bid response as part of this of this Agreement, to undertake the Project, its roll out and sustained operations.

NOW THEREFORE, in consideration of the mutual covenants, promises, assurances, representations and provisions set forth herein, the Parties hereto agree as follows:

i. Definitions

1. **Adverse Effect:** means material adverse effect on
   a) The ability of the System Integrator to exercise any of its rights or perform/discharge any of its duties/obligations under and in accordance with the provisions of this Agreement and/or

The legal validity, binding nature, or enforceability of this Agreement.

1. **Agreement:** means this Agreement/contract together with all Articles, Annexures, Schedules and the contents and specifications of the RFP.
2. **Applicable Law(s):** means any statute, law, ordinance, notification, rule, regulation, judgment, order, decree, byelaw, approval, directive, guideline, policy, requirement or other governmental restriction or any similar form of decision applicable to the relevant party and as may be in effect on the date of the execution of this Agreement and during the subsistence thereof, applicable to the Project.
3. **Application:** means the project or software application developed as a part of scope of work set out in this agreement.
4. **Application Downtime:** means the time for which user/s is not able to access the application. However, in calculating downtime, scheduled downtime (for example, backup time, batch processing time, routine maintenance time) would not be considered.
5. **Assets:** means entire services and software, network or any other information technology infrastructure components used for the Project and other facilities leased/owned/operated by the System Integrator exclusively in terms of ensuring their usability for the delivery of the Services as per this Agreement.

6. **Software:** means the application software/product/customization components designed, developed, tested, and deployed by SI for the purposes of rendering the services and includes the source code along with associated documentation, which is the work product of the development efforts involved in the Project and the improvements effected to such software during the tenure of appointment, on such products, proprietary software components and tools deployed by SI.
7. **Business Hours:** means the working time for PFRDA users which at present is 9:30 AM to 6:00 PM but shall be subject to extension depending upon the work. Cloud or Server and other components which enable successful usage of the software application of PFRDA, the working time should be considered as 24 hours for all the days of the week. It is desired that IT maintenance, other batch processes (like backup) etc. should be planned so that such backend activities have minimum effect on the performance.
8. **Confidential Information:** means all information including PFRDA Data (whether in written, oral, electronic or other format) which relates to the technical, financial and business affairs, dealers, suppliers, products, developments, operations, processes, data, trade secrets, design rights, know-how, plans, budgets and personnel of each Party and its affiliates which is disclosed to or otherwise learned by the other Party in the course of or in connection with this Agreement (including without limitation such information received during negotiations, location visits and meetings in connection with this Agreement);
9. **Deliverables:** means the products, infrastructure and services agreed to be delivered by the System Integrator in pursuance of the agreement as defined more elaborately in the RFP, Implementation and the Maintenance phases and includes all documents related to the user manual, technical manual, design, process and operating manuals, service mechanisms, policies and guidelines (such as security related, data migration related), inter alia payment and/or process related etc., source code and all its modifications;
    a. **PFRDA Data** means all proprietary data of the departments within PFRDA, or its nominated agencies generated out of operations and transactions, and related information including but not restricted to user data which the System Integrator obtains, possesses, or processes in the context of providing the Services to the users pursuant to this Agreement.
    b. **Effective Date:** means the date when this contract starts.
    c. **Force Majeure:** means any event which is unforeseeable, beyond the control of the affected party and materially affects its capacity to perform this Agreement. Such events may include war, civil war, insurrection, riots, revolutions, fire, floods, epidemics, strikes and earthquakes.
    d. **GoI**: means the Government of India.
10. **Intellectual Property Rights (IPR) Clause**
    a. All licenses, software, applications, processes, technologies developed by the SI for the purpose of the project, shall be the exclusive property of PFRDA, on which it will have sole ownership and all attendant rights emanating therefrom, including rights of Intellectual Property. The exclusive rights of PFRDA shall

also extend to the use and ownership of such other licenses, software, applications, processes, technology which belong to SI or sourced by it from a third party, for the exclusive purpose of the project, other than that is specifically excluded by a mutual understanding between the parties. These rights shall be available beyond the original term of the project and SI shall allow the use of the same without any limitations or restrictions.

b. Ownership of Existing Intellectual Property:

- PFRDA acknowledges that the SI may have existing intellectual property rights ("Existing IPR") that are relevant to the project. The SI may retain ownership of all Existing IPR, subject to mutual understanding of the parties, such that right to use by PFRDA shall not be restricted or limited in any manner for the implementation of the project, at all times.

c. New Intellectual Property:

- SI may if required, develop new intellectual property rights ("New IPR") as part of the PFRDA-TRACE. All New IPR, including but not limited to software code, algorithms, documentation, designs, and any other materials developed specifically for the project, shall be the exclusive property of PFRDA.
- PFRDA shall have the sole and exclusive right to use, modify, reproduce, distribute, and otherwise exploit the New IPR without any further rights to the SI, except as explicitly agreed upon in this contract.

d. **License for Pre-existing Third-Party Components:** If the SI uses third-party components or software in the entire project tenure, the SI shall ensure that it or PFRDA obtains any necessary licenses or rights to use such components at no additional cost other than the quoted price in financial bid. Such licenses & any related expenses are to be borne by SI during the entire contract period. PFRDA shall not be responsible for any fees associated with obtaining such licenses during the entire contractual period. SI shall not restrain or withhold itself from procuring and processing such licenses, which shall be detrimental to the smooth implementation of the project.

e. **License for Pre-existing Third-Party Components:** If the SI uses third-party components or software in the entire project tenure, the SI shall ensure that PFRDA obtains any necessary licenses or rights to use such components at no additional cost other than the quoted price in financial bid. Such licenses & any related expenses are to be borne by SI during the entire contract period. PFRDA shall not be responsible for any fees associated with obtaining such licenses during the entire contractual period. SI shall not restrain from processing such licenses, which shall be detrimental to the smooth implementation of the project.

11. **License for Vendor's Tools and Frameworks:** The SI may use its own proprietary tools, frameworks, or methodologies ("SI Tools") in the execution of the project. The SI shall grant PFRDA a non-exclusive, royalty-free, worldwide license to use such Tools solely for the purpose of the project.

12. **Material Breach:** means a breach by either Party (PFRDA or System Integrator) of any of its obligations under this Agreement which has or is likely to have an Adverse Effect on the Project which such Party shall have failed to cure.
13. **Parties:** means PFRDA and System Integrator for the purposes of this Agreement and "Party" shall be interpreted accordingly.
14. **Performance Security**: mean the guarantee provided by SI from a scheduled bank in favour of PFRDA for the performance of its obligations under this Agreement.
15. **Planned Application Downtime:** means the unavailability of the application services due to maintenance activities such as configuration changes, up gradation, or changes to any supporting infrastructure wherein prior intimation (at least two working days in advance) of such planned outage shall be given and approval sought from PFRDA as applicable.
16. **Project:** means the software system as per the Scope of work in RFP or such other modifications to the scope of work and includes the scope outlined in this agreement..
17. **Project Implementation**: means Project Implementation as per the testing standards and acceptance criteria stated in RFP document.
18. **Replacement System Integrator:** means any third party that PFRDA appoint to replace System Integrator upon expiry of the Term or in the event of termination of this Agreement to undertake the provision of Services, as defined hereunder, or part thereof.
19. **Required Consents**: "Required Consents" refer to the consents, waivers, clearances, licenses, and any other authorizations necessary to facilitate the use of PFRDA's Intellectual Property Rights, as defined in Clause XVI, and other permissions that are required by PFRDA or their designated agencies to furnish to the System Integrator in accordance with the terms of this Agreement.
20. **Services:** means the services delivered to the Stakeholders of PFRDA, employees of PFRDA, created, procured, installed, managed, and operated by the System Integrator.
21. **SLA:** means the Performance and Maintenance Service Level Agreement executed by and between PFRDA & SI.
22. **System:** means the System designed, developed/customized, tested and deployed by the System Integrator for the purposes of the Project and includes the source code along with associated documentation, which is the work product of the development efforts involved in the Project and the improvements and enhancements effected during the term of the Project.

23. **Incorporation of Request for Proposal (RFP) into the Master Services Agreement (MSA):** The parties hereby acknowledge and agree that the Request for Proposal (RFP), identified as "Selection Of System Integrator(Si) For Design, Development, Implementation And Maintenance Of PFRDA-TRACE (PFRDA - Tracking Reporting Analytics & Compliance E-Platform)", RFP No. PFRDA/2024/TARCH/PFRDA-TRACE/01, Dated 31st January 2024, and all its terms, conditions, specifications, and responses thereto, shall be deemed to be an integral part of this Master Services Agreement (MSA). Any inconsistencies or ambiguities arising between the RFP and the MSA shall be resolved harmoniously. Both parties shall be bound by the obligations and representations set forth in the RFP, as though they were set forth verbatim in this MSA. The decision of PFRDA shall be final on any interpretation, if required, or on the existence or not of any inconsistency as may be brought by SI, if at all.
24. **Unplanned Application Downtime:** means the total time for all the instances where the application is not available; RFP: means Request for Proposal for "SELECTION OF SYSTEM INTEGRATOR(SI) FOR DESIGN, DEVELOPMENT, IMPLEMENTATION AND MAINTENANCE OF PFRDA-TRACE (PFRDA - TRACKING REPORTING ANALYTICS & COMPLIANCE e-PLATFORM)", RFP No. PFRDA/2024/TARCH/PFRDA-TRACE/01, Dated 31st January 2024, and Addendum/Corrigendum to the Request for Proposal (if any)

    Interpretation

    In this Agreement, unless otherwise specified:

    a. references to a '**company**' shall be construed so as to include any company, corporation, or other body corporate, wherever and however incorporated or established.
    b. references to a **'business day'** shall be construed as a reference to a day (other than a Saturday or Sunday or a public holiday as notified by PFRDA) on which the offices of PFRDA are generally open for business.

The terms "System Integrator" (SI) and "Implementing Agency (IA)" have been used for the same entity i.e., successful bidder selected for the project.

ii. Measurements and Arithmetic Conventions

All measurements and calculations shall be in the metric system and calculations done to 2 (two) decimal places, with the third digit of 5 (five) or above being rounded up and below 5 (five) being rounded down except in money calculations where such amounts shall be rounded off to the nearest INR.

iii. Priority of Documents

This Agreement, including its Schedules and Annexures, represents the entire agreement between the Parties as noted in this Clause. If in the event of a dispute as to the interpretation or meaning of this Agreement it should be necessary for the Parties to refer to documents forming part of the bidding process leading to this Agreement, then such documents shall be relied upon and interpreted in the following descending order of priority:

1. This Agreement
2. The SLA
3. NDA
4. Schedules and Annexures to this agreement.
5. The RFP along with subsequently issued corrigenda.
6. Technical and financial proposal submitted by the successful bidder, in response to the RFP, to the extent they are not inconsistent with any terms of the RFP.

For the avoidance of doubt, it is expressly clarified that any inconsistencies or ambiguities arising between the RFP and the MSA shall be resolved harmoniously in the event of a conflict between this Agreement, Annexures/Schedules or the contents of the RFP, the terms of this Agreement shall prevail over the Annexures/Schedules and Annexures/Schedules shall prevail over the contents and specifications of the RFP.

iv. Basic understanding

SI hereby confirms that:

1. It has fully understood the functions which it has to perform and the obligations it has to discharge as SI as detailed in this Agreement and it acknowledges that this project is very significant to PFRDA in discharge of its powers and functions under the PFRDA Act, 2013.
2. It has the required skills, technical knowledge, qualified personnel, and expertise to carry out its functions and obligations and to provide the services under this Agreement and will build the necessary infrastructure for the purpose.

It possesses the consents of appropriate authorities, licenses, permits and approvals as are necessary for carrying out its functions and obligations under this Agreement.

The parties hereby agree that the above is the basic understanding and based on which PFRDA has entered into this Agreement.

v. Scope of the Project

The broad scope of work of the System Integrator shall be to:

1. Design, develop and implement the project for PFRDA as mentioned in the RFP and in any modifications which may be necessitated for successful implementation of the project.
2. Provide necessary software, infrastructure, and hosting services on MeitY empanelled GCC/VPC.

Provide warranty, AMC, operations, helpdesk, and maintenance support for the period as mentioned in the RFP to ensure successful rollout and acceptance of the system among stakeholders.

Detailed scope of work for the SYSTEM INTEGRATOR is outlined in the RFP document titled **"Selection of System Integrator (SI) for Design, Development, Implementation and Maintenance of PFRDA-TRACE (PFRDA - Tracking Reporting Analytics & Compliance e-Platform)".**

RFP Reference No: PFRDA/2024/TARCH/PFRDA-TRACE/01

vi. Term and Duration of the Agreement

This Agreement shall come into effect on <<dd/mmm/yyyy>> (hereinafter the 'Effective Date') and unless terminated earlier, this agreement shall be in force and effect for a period as defined in RFP. After the end of the contract period, PFRDA reserves the right to either continue with the existing SI with either same or revised terms and conditions as mutually agreed by both parties or assign the work to another SI as it may deem necessary.

vii. Conditions Precedent and Effective Date

Provisions to take effect upon fulfilment of Conditions Precedent

Subject to express terms to the contrary, the rights and obligations under this Agreement shall take effect only upon fulfilment of all the Conditions Precedent set out below. However, PFRDA may at any time at its sole discretion waive fully or partially any of the Conditions Precedent for the System Integrator, without there being any obligations to do so.

Conditions Precedent

The System Integrator shall be required to fulfil the Conditions Precedent which is as follows:

1. to comply with all the conditions stated in RFP, as per the timelines defined in it to provide a Performance Security/Guarantee as stated in to provide PFRDA certified true copies of its constitutional documents and board resolutions authorizing the execution, delivery, and performance of this Agreement by the System Integrator

Extension of time for fulfilment of Conditions

The Parties may, by mutual agreement extend the time for fulfilling the Conditions Precedent and the Terms of this Agreement.

viii. Non-fulfilment of the System Integrator's Conditions Precedent

1. In the event that any of the Conditions Precedent of the System Integrator have not been fulfilled within 30 days of signing of this Agreement and the same have not been waived fully or partially by PFRDA, this Agreement shall cease to exist.
2. In the event that the Agreement fails to come into effect on account of non- fulfilment of the System Integrator's Conditions Precedent, PFRDA shall not be liable in any manner whatsoever to the System Integrator or any third party and PFRDA shall forthwith forfeit the EMD/Performance Security .
3. In the event that possession of any of PFRDA facilities have been delivered to the System Integrator prior to the fulfilment of the Conditions Precedent, upon the termination of this Agreement such shall immediately be reverted to PFRDA, free and clear from any encumbrances or claims.

ix. Representations and Warranties

Representations and warranties of the System Integrator

The System Integrator represents and warrants to PFRDA that:

1. it is duly organized and validly existing under the laws of India and has full power and authority to execute and perform its obligations under this Agreement.
2. it has taken all necessary corporate and other actions under laws applicable to its business to authorize the execution and delivery of this Agreement and to validly exercise its rights and perform its obligations under this Agreement.
3. from the Effective Date, it will have the financial standing and capacity to undertake the Project in accordance with the terms of this Agreement.
4. this Agreement has been duly executed by it and constitutes a legal, valid, and binding obligation, enforceable against it in accordance with the terms hereof, and its

obligations under this Agreement shall be legally valid, binding, and enforceable against it in accordance with the terms hereof.

5. the information furnished in the bid response and as updated on or before the date of this Agreement is to the best of its knowledge and belief, true and accurate in all material respects as at the date of this Agreement.
6. the execution, delivery and performance of this Agreement is not in conflict with, or result in the breach of, or constitute a default by any of the terms of its Memorandum and Articles of Association or any Applicable Laws or any covenant, contract, agreement, arrangement, understanding, decree, or order to which it is a party.
7. it has complied with Applicable Laws in all material respects and has not been subject to any fines, penalties, injunctive relief or any other civil or criminal liabilities which in the aggregate have or may have an Adverse Effect on its ability to perform its obligations under this Agreement; and
8. no sums, in cash or kind, have been paid or shall be paid, by it or on its behalf, to any person by way of fees, commission or otherwise for entering into this Agreement or for influencing or attempting to influence any officer or employee of PFRDA in connection therewith.

Representations and warranties of PFRDA

PFRDA represent and warrant to the System Integrator that:

1. It has taken all necessary actions under Applicable Laws to authorize the execution, delivery, and performance of this Agreement and to validly exercise its rights and perform its obligations under this Agreement.
2. This Agreement has been duly executed by it and constitutes a legal, valid, and binding obligation enforceable against it in accordance with the terms hereof and its obligations under this Agreement shall be legally valid, binding, and enforceable against it in accordance with the terms thereof; and
3. All information provided by it in the RFP in connection with the Project is, to the best of its knowledge and belief, true and accurate in all material respects.

x. Obligations of PFRDA

Without prejudice to any other undertakings or obligations of PFRDA under this Agreement, PFRDA shall perform the following:

1. To authorize the System Integrator to interact for implementation of the Project with external entities such as the MeitY empanelled GCC/VPC, System Integrators, SMS/Email Gateway System Integrators etc.

To provide the data in the template designed by SI in excel/word format for the purpose of data migration.

xi. Obligations of the System Integrator

The following forms illustrative obligations of System Integrator:

1. All data, information, output generated from using the system provided by SI under this project shall be the exclusive property of PFRDA on which it alone shall have ownership and will not be used by SI or any of its employees, affiliates or third parties in any manner without the prior permission of PFRDA, either for any commercial or non-commercial purposes.
2. System Integrator shall be solely responsible for the performance and completion of all its obligations.
3. It shall provide to PFRDA, the deliverables as set out in RFP document or as modified within the specified timelines. Both the timelines and quality delivery, in a cost-effective manner, shall be an essence of this project and this contract .
4. It shall perform the Services as set out in RFP so as to comply with the applicable Service Levels set out with this Agreement.
5. It shall ensure that the Services are being provided as per the Project Timelines set out in RFP.
6. System Integrator will abide by the job safety measures prevalent in India and will free PFRDA from all demands or responsibilities arising from accidents or loss of life, the cause of which is System Integrator's negligence. System Integrator will pay all indemnities arising from such incidents and will not hold PFRDA responsible or obligated.
7. System Integrator shall be obliged to give timely and sufficient support to PFRDA's staff, work closely with PFRDA's staff, act, and abide by directives issued by PFRDA that are consistent with the terms of the Agreement and the RFP. System Integrator shall be responsible for managing the activities of its personnel and will hold itself responsible for any misdemeanours.
8. System Integrator shall be responsible for and obligated to conduct all contracted activities with due care and diligence, in accordance with this Agreement and using state-of-the-art methods and exercising all reasonable means to achieve the performance specified in this Agreement.
9. Whenever any designated personnel's of System Integrator are leaving his job, System Integrator shall immediately inform the same on receipt and give prior information about this to PFRDA and provide suitable alternative personnel to the satisfaction of PFRDA
10. System Integrator's engineer(s) shall not change the password of network, security devices/applications software/tools without the knowledge of PFRDA's Team. In case they are aware about any password(s), they shall not share it with anyone other than PFRDA's team without prior written approval from PFRDA's Team.

11. If necessary, PFRDA may escalate the call to higher authorities of System Integrator. In that case, System Integrator shall put their maximum efforts and deploy their best resources to resolve the calls at the earliest possible time frame at all locations and ensure appropriate uptime.
12. System Integrator shall be responsible for any or all act of its employees that may result in security breach of confidentiality or any other breach under this agreement or in terms of this RFP.
13. System Integrator shall assign personnel of appropriate qualifications and experience to perform the services in order to fulfil its obligations.
14. System Integrator shall exercise requisite control and supervision over its personnel in the course of rendering the services and make best efforts to ensure that the services are rendered in a continuous and uninterrupted manner.
15. System Integrator shall always respect the confidentiality of all information given to it by PFRDA and shall not divulge such information to any third party or other units without the prior written consent of PFRDA.
16. System Integrator shall promptly install/implement the corrected licensed software and/or maintenance releases/updates at no additional cost or fees or expenses.
17. System Integrator shall undertake regular preventive maintenance of the licensed software.
18. All bug fixations/modifications/enhancements relating to the licensed software shall be done by System Integrator in a time bound manner as per the SLA. The System Integrator shall adopt a common, smooth, timely, effective and satisfactory bug/enhancement handling mechanism.
19. System Integrator is obliged to work closely with PFRDA's staff, act within its own authority and abide by directives/instructions issued by PFRDA from time to time.
20. System Integrator shall be required to develop, maintain, and manage the proposed services to enable PFRDA to meet its requirements. It shall be System Integrator's responsibility to ensure compliance to the requirements of the continued operation of the intended services in accordance with and in strict adherence to the terms of its Bid, the RFP, and this Agreement.
21. In addition to the aforementioned, System Integrator shall ensure that System Integrator's Team is competent, professional and possesses the requisite qualifications and experience appropriate to the task they are required to perform under this Agreement. System Integrator shall ensure that the Services are performed through the best efforts of System Integrator's Team, in accordance with the terms hereof and as per Acceptance Criteria as stated in the RFP. Nothing in this Agreement shall be considered to relieve System Integrator from its liabilities or obligations under this Agreement to provide the Services in accordance with PFRDA's directions and requirements and as stated in this Agreement and the Bid to the extent accepted by PFRDA and System Integrator shall be liable for any non-performance, non-compliance, breach or other loss and damage resulting either directly or indirectly by or on account of its Team.

22. All personnel so employed/engaged by System Integrator shall at all times be the employees of System Integrator under all statutes and in case any dispute arises between such personnel and System Integrator, it shall be resolved and settled between them. System Integrator agrees and undertakes that in no way System Integrator shall involve PFRDA in any of their grievances and/or disputes. System Integrator undertakes to indemnify PFRDA against any and all claims, proceedings, actions, damages, losses, costs, and expenses arising out of a) such grievances or disputes b) noncompliance of applicable law. c) non- payment/delays in payment of dues of its employees d) settlement/payments of any claim or compensation or dues pertaining to employees of System Integrator d) cost of litigation, proceeding including fees of legal professionals engaged by PFRDA for defending or responding or pursuing such litigation/proceedings. System Integrator shall maintain all books and records as are required to be maintained under the applicable rules, regulations and laws including muster roll, wage register, leave register etc. and System Integrator shall be solely and personally responsible and liable for the breach of any or all of the statutory obligations in respect of all its employees etc. engaged under this Agreement and PFRDA shall in no way be held responsible for any breach committed by System Integrator in this regard.
23. PFRDA shall not be held liable or responsible for any claim (monetary or otherwise), damage (of any kind) or liability suffered by System Integrator and/or its employees/contractors, employed/engaged for providing services under this Agreement. System Integrator undertakes that no claim/dispute shall be raised against PFRDA by contractors or employees engaged by the System Integrator.
24. System Integrator shall supply to PFRDA, at least 10 (ten) days prior to the effective date of commencement of works/services or kick-off meeting whichever is earlier, an organization chart showing the proposed organization/manpower to be established by System Integrator for execution of the work/facilities/services including the identities and Curriculum-Vitae of the key personnel to be deployed. System Integrator shall inform PFRDA in writing in advance, of any revision or alteration of such organization charts.
25. System Integrator shall be responsible for the deployment, transportation, accommodation, and other requirements of all its employees required for the execution of the work and for all costs/charges in connection thereof or incidental thereto.
26. System Integrator shall provide and deploy, onsite for carrying out the work, only those manpower resources who are skilled and experienced in their respective trades and who are competent to execute or manage/supervise the work in a proper and timely manner.

27. PFRDA may at any time object to and require the System Integrator to remove forthwith from on-site a supervisor or any other authorized representative or employee of the System Integrator or any person(s) deployed by System Integrator, if, in the opinion of PFRDA the person in question has misconducted himself. System Integrator shall forthwith remove and shall not again deploy the person in question at the work site without the prior written consent of PFRDA's Representative.
28. PFRDA may at any time direct System Integrator to remove from the work/Site System Integrator's supervisor or any other authorized representative including any employee of System Integrator, or any person(s) deployed by System Integrator for professional incompetence or negligence or for being deployed for work for which he is not suited. System Integrator shall take necessary steps to remove that person from deployment on the work, which System Integrator shall then forthwith do and shall not again deploy any person so objected to on the work or on the sort of work in question (as the case may be) without the written consent of PFRDA.
29. System Integrator shall maintain backup personnel and shall promptly provide replacement of every person removed, pursuant to this section, with an equally competent substitute from the pool of backup personnel.
30. In case of change in its team composition owing to attrition, System Integrator shall ensure seamless activities to ensure proper knowledge transfer and handover/takeover of documents and other relevant materials between the outgoing and the new member without adversely affecting the execution of the project. The exiting team member should be replaced with an equally competent substitute from the pool of backup personnel. System Integrator shall ensure that the project or services should not be adversely affected due to any change in team deployed/engaged to provide Services under this Agreement.
31. System Integrator shall comply with the provision of all laws including Information Technology Act (as amended), labour laws, rules, regulations, and notifications issued there under from time to time. System Integrator shall comply with all norms relating to data protection including the Digital Personal Data Protection Act, 2023 or any law or rules or regulations that may be in force during the term of this Agreement. All safety and labour laws enforced by statutory agencies and by PFRDA shall be applicable in the performance of this Agreement and System Integrator shall abide by these laws.
32. System Integrator shall promptly but not later than two days, report to PFRDA any evidence, which may indicate or is likely to lead to an abnormal or dangerous situation and shall take all necessary emergency control steps to avoid such abnormal situations.
33. System Integrator shall also adhere to all security requirement/regulations of PFRDA during the execution of the work.
34. System Integrator and its employees shall always adhere to internal security and safety policies of PFRDA.

35. System Integrator shall put all efforts to ensure that no Computer Virus, Spyware, ransomware is introduced onto PFRDA's or any user's computer equipment or systems by any act, omission or negligence of System Integrator or its employees. The User shall mean any entity using services, software, systems etc. provided by PFRDA or licensed to PFRDA.
36. All other obligations of the SI not specifically mentioned under this agreement, shall be exactly as per the other terms and conditions of this RFP (to be fulfilled by the successful bidder), which shall be treated an integral part of this agreement.

xii. **Approvals and Required Consents**

PFRDA shall use reasonable endeavours to assist System Integrator to obtain the Required Consents. In the event that any Required Consent is not obtained, the System Integrator and PFRDA will co- operate with each other in achieving a reasonable alternative arrangement as soon as reasonably practicable for PFRDA to continue to process its work with as minimal interruption to its business operations as is commercially reasonable until such Required Consent is obtained, provided that the System Integrator shall not be relieved of its obligations to provide the Services and to achieve the Service Levels until the Required Consents are obtained, such that execution of the project is neither delayed nor adversely affected in any other manner.

xiii. **Financial Matters**

a) Terms of Payment and Service Credits and Debits

1. In consideration of the Services and subject to the provisions of this Agreement and of the SLA, PFRDA shall pay the System Integrator for the Services rendered successfully and to the satisfaction of PFRDA in pursuance of this agreement, in accordance with the Payment Milestones set out in this Agreement.

All payments shall be made to the System Integrator subject to the application of liquidated damages/ compensation and/or SLA as per Terms and Conditions defined in the RFP.

b) Invoicing and Settlement

Subject to the specific terms of the SLA, the System Integrator shall submit its invoices in accordance with the following principles:

1. PFRDA shall be invoiced by the System Integrator for the Services. Generally, and unless otherwise agreed in writing between the Parties or expressly set out in the SLA, the System Integrator shall raise an invoice; and
2. Payment shall be made within 30 working days of the receipt of invoice along with supporting documents by PFRDA subject to deductions, where applicable on account of default.

3. PFRDA shall be entitled to delay or withhold payment of any invoice or part of it delivered by the System Integrator. which is in dispute. Endeavour shall be made by PFRDA to settle all bills and make payment within the time period. The disputed/withheld amount shall be settled post resolution of the dispute. Further, the System Integrator will not claim any interest on the arrear/payment due but not paid by PFRDA. Any exercise by PFRDA under this Clause shall not entitle the System Integrator to delay or withhold provision of the Services.

c) Performance Security

1. The Performance Security is required to protect the interest of PFRDA against delay in supply/installation and/or the risk of non- performance by the Si and to secure successful implementation of the project, or performance of the material or services sold, or , or seek required damages/compensation for any breaches stipulated, which may warrant invoking of Performance Security.
2. Performance Security shall be 10% of the total Contract value. Performance Security may be submitted in the form of a Performance Security (PS) for the amount with validity period as specified in the RFP strictly as per the format at **Appendix- II**. The Performance security has to be issued by a Scheduled Commercial Bank and needs to be submitted within the specified time of receipt of formal communication from PFRDA about SI's Bid finally selected .The Performance Security may need to be extended accordingly depending on the extension of the Contract period. Performance security may also be submitted in the form of Fixed Deposit Receipt - issued by a Scheduled Commercial bank lien marked in favour of PFRDA and should be valid up to 180 days from the date of completion of the contract. The Fixed deposit may need to be extended accordingly depending on the extension of the Contract period.

xiv. **Termination of the contract**

(1) This contract may be terminated by PFRDA at any time upon the happening of any of the following events and shall be without prejudice to any other action on the part of PFRDA:

(i) If the SI is in breach of any of the terms and conditions of this contract being a breach which in opinion of PFRDA is reasonably capable of remedy and where PFRDA serves notice on the SI specifying the breach and the SI fails to satisfactorily remedy such breach within 30 days after the service of such notice. Notwithstanding the said clause, PFRDA in the event of happening of any of violations/breaches according to it, may terminate the contract by giving a prior notice of 90 days in which case it shall not be necessary to give any opportunity to the SI to remedy the breach.

(ii) If the SI shall be in material breach of any of the terms and conditions of this contract (including the basis on which SI was selected) being a breach which in

opinion of PFRDA is not reasonably capable of remedy, by giving 90 days' notice.

(iii) If by reason of any order/policy of a government or other authority the continued operation and performance of this contract and all its provisions in a material respect is prevented, discontinued, or is delayed for any unspecified and indeterminate period or is rendered impossible on account of any other reason.

(iv) If the SI is not able to perform its duties and obligations, consistently, despite specific opportunities granted to it such that in the opinion of PFRDA, the SI is not capable of performing the contract effectively.

(v) If the SI becomes insolvent or goes into either voluntary or compulsory liquidation or closure (except amalgamation or reconstruction provided that the emergent company affirms its adherence to the terms and conditions of the Agreement) or a Receiver or Manager is appointed in respect of the whole or part of SI or enter into any arrangement with its creditors either by composition or otherwise.

(vi) If in the opinion of PFRDA, the SI has been found to be indulging in corrupt practices or has obtained the award of the contract based on submission of false or incorrect information and documents or has been blacklisted by any government authority on the above grounds.

(2) Besides the above, PFRDA reserves the right to terminate the agreement with the SI by giving the SI a notice of 90 days (with or without assigning any reason) if PFRDA decides that the services of the SI will no longer be required or PFRDA decides not to go ahead with the project, at all or in any other modified form. In such a case, PFRDA shall reimburse the actual expenses incurred by the SI for providing the deliverables.

(3) SI shall be entitled to terminate the contract, where PFRDA delays in making payments (which is not in dispute) beyond a period of 180 days, from which it becomes due for payment.

(4) Notwithstanding any period specified under this clause, the SI shall be required and liable to perform its obligations as per exit management plan and the contract shall be deemed to be in force only for such limited purpose to implement the exit management plan.

(5) If the Contract is terminated, SI shall handover all documents/executable/Authority's data or any other relevant information to PFRDA in timely manner and in proper format as per scope of this contract/RFP and shall also support the orderly and seamless transition to another party/SI chosen by PFRDA or to PFRDA.

(6) PFRDA's right to terminate the agreement/contract will be in addition to the right of seeking compensation and/or liquidated damages and other actions as may be deemed appropriate, besides PFRDA shall have the right to forfeit the Performance security in the event of breach or shortcomings on the part of SI or any loss caused to PFRDA, due to acts of omission or commission on the part of SI, without there being any requirement to prove the exact amount of loss. PFRDA shall also have the right to call upon SI to extend the performance security by such time period as may be required to protect its

rights or to secure the obligations of SI and to also replenish the performance security, where part of it is forfeited.

xv. Indemnity

1. SI shall indemnify, protect, save, and hold PFRDA harmless from and against all claims, losses, costs, damages, expenses, action suits and other proceedings, (including reasonable attorney fees), relating to or resulting directly or indirectly from:
    a. an act or omission of SI, its employees, its agents in the performance of the services provided by this contract, breach of any of the terms of this RFP or breach of any representation or warranty, use of the deliverables and/or services provided by SI.
    b. Infringement of any patent, trademarks, copyrights etc. or such other statutory infringements in respect of all components provided to fulfil the scope of this project.
    c. Any loss or damage arising out of loss of data, breach of data privacy and third-party claims on PFRDA for malfunctioning of the equipment or software or deliverables at all points of time, provided however, PFRDA notifies SI in writing in a reasonable time frame on being aware of such claim. SI has sole control of defence and all related settlement negotiations, PFRDA provides SI with the assistance, information, and authority as it deems fit to perform the above.
    d. SI shall in no event enter into a settlement, compromise or makes any statement (including failure to take appropriate steps) that may be detrimental to PFRDA's (and/or its stakeholders, users, and SIs) rights, interest, and reputation.
    e. SI shall be responsible for any loss of data, loss of life, etc. due to acts of SI's representatives, and not just arising out of gross negligence or misconduct, etc. as such liabilities pose significant risk.
    f. SI should take full responsibility for its and its employee's actions. Further, since PFRDA's data could be integrated/used under SI provided software, bidder should be responsible for loss/compromise or damage to PFRDA's data and for causing reputation risk to PFRDA.
    g. SI should indemnify PFRDA (including its employees, members, or representatives) from and against claims, losses, liabilities, penalties, fines, and suits arising from:
    h. IP infringement under any laws including Copyrights Act 1957 or IT Act 2000 and such other statutory acts and amendments thereto.
2. Negligence and misconduct of SI, its employees, and agents.
3. Breach of any terms of RFP, Representation or Warranty, this agreement or SLA.
4. Act or omission in performance of service.

Loss of data due to any of the reasons mentioned above or violation of confidentiality clause.

5. Non-compliance of SI with Laws/Governmental/regulatory Requirements
    a. In the event that PFRDA is called as a defendant for IPR infringement of patent, trademark or industrial design rights arising from use of any of the components of the supplied solution, SI on its own expense shall undertake to defend PFRDA fully.
    b. It will be SI's responsibility to rapidly do away with such third-party claims. SI will also pay any compensation arising from the infringement claims and PFRDA will in no manner be responsible for such payments. In addition, SI shall bear all the related expenses and legal fees.
    c. On its part, PFRDA may immediately relay to SI any such claims and help within reasonable limits to rid the claim.
    d. SI must undertake that all the components delivered re free of defects, are brand new and original. If at some stage it is discovered that the components do not meet these criteria, PFRDA has the right to cancel the respective order and SI shall indemnify and refund the total amount received from PFRDA along with compensation. Similar conditions apply to software; as well the system software must be licensed and original.
6. System Integrator shall be liable to indemnify PFRDA, at its own cost and expenses, against all losses/damages, which PFRDA may suffer on account of violation by System Integrator of any or all national/international laws, norms, standards, procedures etc. in relation to provision of services and deliverable under this Agreement.
7. SI shall be solely responsible for and shall indemnify and keep PFRDA, its employees, agents, officers, and members indemnified and harmless from and against all costs (including but not limited to litigation expenses and attorney's fees), expenses, losses, liabilities, fines, penalties, damages, claims, demands, actions, or proceedings whatsoever for arising out:
    a. any death or personal injury caused by any act or omission of System Integrator, its employees, or agents. Any third-party claims for infringement of a copyright, patent, trademark or other intellectual property right of any third-party including claims made by agents of the System Integrator against PFRDA for any breach committed by the System Integrator in relation to such third parties.
    b. Notwithstanding the foregoing, System Integrator shall not be obliged to indemnify PFRDA for any fault/shortcomings directly attributable to PFRDA.

xvi. **Termination for Convenience**

PFRDA, by written notice of not less than 90 (ninety) days, may terminate the Contract, in whole or in part without assigning any reason. In the event of such termination, PFRDA shall only be liable to provide payment for the Services rendered (delivered) up to the effective date of termination. In such circumstances SI shall provide all necessary assistance to PFRDA or other SI, so that the project is not adversely affected in any manner.

xvii. Effects of Termination

1. Upon termination of this Agreement, the Parties will comply with the Exit Management clause as specified in this Agreement.
2. If the termination is initiated before go-live, the financial settlement for the system integrator will be calculated on the basis of approved/signed off deliverables.
3. If the exit management is initiated post go-live, the financial settlement for the system integrator will be calculated on the basis of service provided during the warranty or operations and maintenance phase as applicable.

xviii. Minimum Wages

SI hereby agrees and undertakes that during the subsistence of this agreement it will not employ any personnel/individual below the Minimum Wages fixed by appropriate Government on this behalf from time to time, as per the provisions of applicable Minimum Wages law. In this effect, SI has to submit undertaking on their company letterhead signed by authorized signatory.

The SI will ensure strict compliance of all labour laws, insurance, minimum wages to the staff employed/deployed/engaged for the work assigned and PFRDA will not be liable for any such persons/personnel of successful bidder and shall not be liable for any levies/penalties etc. that may be imposed by the Authorities concerned for their action/inaction. There shall be no employer employee relationship whatsoever between PFRDA and the SI, their employees and SI or its employees, staff, agents will not be entitled to any employment with PFRDA. In the event of any demand/fines/Compensation made by any of the authorities on PFRDA in respect of the conduct/actions taken by SI/their employees/labourers, PFRDA will be entitled to recover the said amounts from the bills/amount payable or from the performance guarantee and also take appropriate action against said persons of SI for their misconduct.

xix. Exit Management

Where PFRDA intends to continue equivalent or substantially similar services to the Services provided by System Integrator after termination or expiry of this Agreement, either by performing them itself or by means of a contract with New/Replacement SYSTEM INTEGRATOR, the System Integrator herein shall ensure the smooth transition to the Replacement SYSTEM INTEGRATOR and shall co-operate with PFRDA, or the Replacement SYSTEM INTEGRATOR as required in order to fulfil the obligations.

System Integrator shall co-operate fully with PFRDA and shall provide sufficient information to comply with the reasonable requests of PFRDA to enable an effective tendering process to take place for selection of new SI.

System Integrator shall comply with all reasonable requests by PFRDA to provide information relating to the operation of the Services, including but not limited to, services and software

used, inter-working, coordinating with other application owners, access to and provision of all performance reports, agreed procedures, and any other relevant information (including the configurations set up for PFRDA and procedures used by System Integrator for handling Data) reasonably necessary to achieve an effective transition.

System Integrator shall provide to PFRDA an analysis of the Services to the extent reasonably necessary to enable PFRDA to plan migration of such workload to a Replacement SYSTEM INTEGRATOR.

System Integrator shall co-operate with PFRDA during the handover to a Replacement SYSTEM INTEGRATOR and such co-operation shall extend to, but shall not be limited to, inter-working, coordinating and access to and provision of all operational and performance documents, reports, summaries produced by System Integrator for PFRDA, including the configurations set up for PFRDA and any and all information to be provided by System Integrator to PFRDA under any other term of this Agreement necessary to achieve an effective transition without disruption to routine operational requirements.

The exit by SI would be considered as complete only upon completing all these requirements as given in this exit management document based on which final payment and all other matters will be settled. Compliance with exit management plan by SI, shall be an essence of this agreement.

Non-adherence to exit management plan by SI in any manner, will entitle PFRDA to seek such further damages and compensation, above the sums stipulated in this agreement, considering that continuity is required to be maintained of the project, even when the SI ceases to be part of the project, by expiry of the agreement or earlier termination thereof. SI shall be liable to compensate PFRDA on a per day basis or in any other manner, for breach on its part in implementing the exit management.

Notwithstanding the above, PFRDA shall be entitled to seek such remedial measures as may be warranted to secure the satisfactory performance of the SI in implementing the exit management, such that the project is not adversely affected on account of lack of continuity.

xx. Transfer of Configuration Management Database

Six (6) months prior to expiry or within 2 (two) months of notice of termination of this Agreement System Integrator shall deliver to PFRDA a full, accurate and up to date cut of content from the Configuration Management Database (or equivalent) used to store details of Configurable Items and Configuration Management data for all products used to support delivery of the Services.

xxi. Transfer of Assets

1. Six (6) months prior to expiry or within 2 (two) months of notice of termination of the Agreement System Integrator shall deliver to PFRDA the Asset Register comprising of:
2. a list of all Assets eligible for transfer to PFRDA; and
3. a list identifying all other Assets, (including human resources, skillset requirement and know-how), that are essential to the delivery of the Services.
4. Within 1 (one) month of receiving the Asset Register as described above, PFRDA shall notify System Integrator of the Assets it requires to be transferred, (the "Required Assets"), and PFRDA and System Integrator shall provide for the approval of PFRDA a draft plan for the Asset transfer.

xxii. Transfer of Software Licenses

1. Six (6) months prior to expiry or within 2 (two) months of notice of termination of this Agreement System Integrator shall deliver to PFRDA all licenses for Software used in the provision of Services which were purchased by/for PFRDA.
2. On notice of termination of this Agreement System Integrator shall, within 2 (two) months of such notice, deliver to PFRDA details of all licenses.

xxiii. Transfer of Software & Cloud & related services

Wherein PFRDA is the owner of the software, Six (6) months prior to expiry or within 2 (two) months of notice of termination of this Agreement System Integrator shall deliver, or otherwise certify in writing that it has delivered, to PFRDA a full, accurate and up to date version of the Software including up to date versions and latest releases of, but not limited to:

1. Source Code and associated documentation.
2. Application architecture documentation and diagrams.
3. Release documentation for functional, technical and interface specifications.
4. Plan with allocated resources to handover code and design to new development and test teams (this should include architectural design and code 'walk-through').
5. Source Code and supporting documentation for testing framework tool and performance tool.
6. Test results for the latest full runs of the testing framework tool and performance tool on each environment.
7. Cloud migration plan with SOP for BCP.

xxiv. Transfer of Documentation

Six (6) months prior to expiry or within- 2 (two) months of notice of termination of this Agreement System Integrator shall deliver to PFRDA a full, accurate and up-to date set of Documentation and approvals that relates to any element of the Services.

xxv. Transfer of Service Management Process

Six (6) months prior to expiry or within 2 (two) months of notice of termination of this Agreement System Integrator shall deliver to PFRDA but not limited to:

1. a plan for the handover and continuous delivery of the Service full and up to date, both historical and outstanding Service Desk ticket data including, but not limited to:
2. Incidents.
3. Problems.
4. Service Requests.
5. Changes.
6. Service Level reporting data.
7. List and topology of all tools and products associated with the provision of the Software and the Services.
8. Full content of software builds and server configuration details for software deployment and management, and monitoring software tools and configuration.

xxvi. Transfer of Knowledge Base

Six (6) months prior to expiry or within 2 (two) months of notice of termination of this Agreement System Integrator shall deliver to PFRDA a full, accurate and up to date cut of content from the knowledge base (or equivalent) used to troubleshoot issues arising with the Services but shall not be required to provide information or material which System Integrator may not disclose as a matter of law.

xxvii. Transfer of Service Structure

Six (6) months prior to expiry or within 2 (two) months of notice of termination of this Agreement System Integrator shall deliver to PFRDA a full, accurate and up to date version of the following, as a minimum archive of records

1. Programme plan of all work in progress currently accepted and those in progress.
2. Latest version of documentation set.
3. Source Code (if appropriate) and all documentation to support the services build tool.
4. Source Code, application architecture documentation/diagram and other documentation.

5. Project plan and resource required to hand Service Structure capability over to the new team.

xxviii. Training Services on Transfer

1. System Integrator shall comply with PFRDA's reasonable request to assist in the identification and specification of any training requirements following expiry or termination. The purpose of such training shall be to enable PFRDA or a Replacement SYSTEM INTEGRATOR to adopt, integrate and utilize the Data and Assets transferred and to deliver an equivalent service to that previously provided by System Integrator.
2. System Integrator shall produce for PFRDA's consideration and approval Six (6) months prior to expiry or within 2 (two) months working days of issue of notice of termination:
3. A training strategy, which details the required courses and their objectives.
4. Training materials (including assessment criteria); and
5. a training plan of the required training events.
6. System Integrator shall schedule all necessary resources to fulfil the training plan and deliver the training.

xxix. Transfer Support Activities

1. Six (6) months prior to expiry or within 2 (two) months of issue of notice of termination, System Integrator shall assist PFRDA or Replacement SYSTEM INTEGRATOR to develop a viable exit transition plan which shall contain details of the tasks and responsibilities required to enable the transition from the Services provided under this Agreement to the Replacement SYSTEM INTEGRATOR or PFRDA, as the case may be.
2. The exit transition plan shall be in a format to be agreed with PFRDA and shall include, but not be limited to:
    a. Timetable of events
    b. Resources
    c. Assumptions.
    d. Activities.
    e. Responsibilities
    f. Risks.
    g. System Integrator shall supply to PFRDA or a Replacement SYSTEM INTEGRATOR specific material including but not limited to:
    h. Change Request log.
    i. Entire back-up history.
    j. Incident logbook
    k. Asset Register, problem management system and operating procedures

l. On the date of expiry System Integrator shall provide to PFRDA refreshed versions of the materials which shall reflect the position as at the date of expiry.

xxx. Training, handholding, and knowledge transfer

1. The System Integrator shall hold technical knowledge transfer sessions with designated team of PFRDA and/or any designated agency in the last three (03) months of the project duration.
2. The System Integrator shall hold operational hand-holding sessions on the Application software with the designated officers/staff members of PFRDA, so that PFRDA can continue with the application even after System Integrator exits the project.

xxxi. Limitation of Liability

1. System Integrator shall not be liable or responsible for any delay or failure to perform the Services or failure of the Services or a Deliverable to the extent that such delay or failure has arisen as a result of any direct delay or failure by PFRDA to perform any of its obligations (other than payment of disputed amounts) which directly affects the performance of SI, or its obligations, for lack of clarity or decision to be given by PFRDA. In the event that SI is delayed or prevented from performing its obligations due to such failure or delay on the part of or on behalf of PFRDA, then the SI may be allowed an additional period of time to perform its obligations and unless otherwise agreed the additional period shall be equal to the amount of time for which SI is delayed or prevented from performing its obligations due to such direct failure or delay on the part of or on behalf of PFRDA. Such failures or delays shall be brought to the notice of PFRDA, immediately within two (02) days of occurrence of such failures or delays and subject to mutual agreement with PFRDA, the SI shall take such actions as may be necessary to correct or remedy the failures or delays such that performance of the project is not adversely affected.
2. Notwithstanding anything contained in this Agreement the total cumulative liability of SI/either partly arising from or relating to this Contract shall not exceed the total amount paid to the SI by PFRDA under this Agreement (excluding the taxes, reimbursements etc.) provided, however, that this limitation shall not apply to any liability for damages/compensation arising from breach of SI's obligations affecting the project adversely to the detriment of PFRDA (a) wilful default/deliberate inaction/fraud by SI or (b) indemnification claims by third party for infringement against PFRDA.

xxxii. Force Majeure

1. Notwithstanding the provisions of terms and conditions contained in the RFP and or Agreement, neither party shall be liable for any delay in performing its obligations herein if and to the extent that such delay is the result of an event of Force Majeure.

2. For the purposes of this clause, 'Force Majeure' means and includes wars, insurrections, revolution, civil disturbance, riots, terrorist acts, public strikes, bundh, fires, floods, epidemic, Vis Major, acts of Government in their sovereign capacity, but does not include any foreseeable events, commercial considerations or those involving fault or negligence on the part of the party claiming Force Majeure.
3. If a Force Majeure situation arises, System Integrator shall promptly notify PFRDA in writing of such condition and the cause thereof. Unless otherwise directed by PFRDA in writing, System Integrator shall continue to perform its obligations under the Contract as far as is reasonably practical and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event.
4. If the force majeure situation persists for an indefinite period, beyond 60 days, the parties shall consult each other on further actions necessary to salvage the project.

xxxiii. Notices

Any notice given by one party to the other pursuant to this Contract shall be sent to other party in writing and to be confirmed in writing to other Party's address. The notice shall be effective when delivered or on the notice's effective date whichever is later.

xxxiv. Confidentiality

Subject to the NDA executed between the parties, In the course of performing its functions and obligations under this Agreement, System Integrator shall maintain strict secrecy, confidentiality and privacy in respect of the confidential records and information that has come to its possession or knowledge.

1. System Integrator shall keep utmost confidentiality of the details and information with regard to the Project, including systems, facilities, operations, management, and maintenance of the systems.
2. It is agreed between PFRDA and System Integrator that PFRDA has a right to prevent or prohibit System Integrator at any time from disclosing any information and records to any person and System Integrator shall abide by such decision and when disclosure is required or by due process of law it shall give prior notice to PFRDA.
3. System Integrator agrees that it shall ensure that all its employees, agents, System Integrators and any another related stakeholder are bound by nondisclosure agreement and shall provide the same as per the terms stated in RFP.

xxxv. Liquidated Damages/Compensation

If the System Integrator fails to deliver product/services satisfactorily within the stipulated time schedule as specified in this RFP/Agreement, or as may be modified, PFRDA may, without prejudice to its other remedies under the RFP/Agreement, and unless otherwise extension of time is agreed upon (without the application of liquidated damages/compensation), deduct from

the Project Cost, such liquidated damages/take compensation as defined in SLA and compensation at ***Appendix-IV.*** Once the maximum deduction is reached, PFRDA may consider termination of the Agreement. This shall be without prejudice to rights of PFRDA to terminate the contract at any time, if the SI is in breach of its obligation such that the project is being adversely affected in the opinion of PFRDA. This liquidated damages/compensation may also be adjusted from any payment due to be given to SI, or from the performance security submitted by SI or PFRDA may directly notify SI to pay the same.

1. PFRDA expects that SI completes the scope of work within the timeframe. Inability of SI to either provide the requirements as per the scope or to meet the timelines as specified would be treated as breach of contract and would invoke the liquidated damages/compensation clause. In case of the Go-Live delays by SI the compensation as per PFRDAs calculation will be imposed on SI of 5% of the total contract value per month of delay, to the maximum of 10% of the total contract value.
2. Thereafter, at the discretion of PFRDA, the contract may be cancelled (if this more than 1 quarter). PFRDA may also invoke the Performance Guarantee, seek compensation on delay which is not attributable to it and is attributable to SI.
3. SI should ensure implementation of the software application with all the functional, technical and security requirements as specified in the RFP document.
4. Notwithstanding anything contained above, no such compensation will be chargeable on SI for the inability occasioned, if such inability is due to reasons entirely attributable to PFRDA.
5. Compensation payable by SI will be recovered from the bills. No payment due will be released/adjusted before compensation due is paid by SI.
6. There would be no payment for man-days invested in removing defects in developments.
7. In case of non-replacement of resource within two weeks after the release of existing resource, a compensation of Rs. 10,000/- per day will be payable till the new and suitable resource is provided. The waiver may be permitted by PFRDA subject to the conditions that may be imposed to ensure that the project is not jeopardized.
8. The compensation is payable at the rate of 10% of the annual payment for each instance of violation if SI fails to protect data breach and violates confidentiality of information.
9. Total compensation of the project should not increase more than 10% of the TCO.
10. Non-adherence to exit management plan by SI in any manner, will entitle PFRDA to seek such further damages and compensation, above the sums stipulated in this agreement, considering that continuity is required to be maintained of the project, even when the SI ceases to be part of the project, by expiry of the agreement or earlier termination.

xxxvi. Intellectual Property Rights and Ownership Provisions :

1. Ownership of Custom Software/Customizations: All Custom Software or customizations developed exclusively for PFRDA under this Agreement shall be

deemed works made for hire. PFRDA shall exclusively own all rights, title, and interest worldwide in such Custom Software or customizations, including all associated intellectual property rights.

2. Waiver of Moral Rights: The Solution Integrator (SI) and its representatives expressly waive any moral rights in the Custom Software developed under this Agreement.
3. Assistance in Securing Rights: The SI shall provide PFRDA with all necessary assistance, including executing documents or directing its employees to do so, to secure rights related to any Custom Software, such as patent or copyright applications.
4. Acknowledgement of SI's Proprietary Materials: PFRDA recognizes that the SI may use proprietary materials in performing services, which remain the SI's intellectual property. However, if such materials are embedded in the deliverables, the SI grants PFRDA a non-exclusive license for its use without any other cost on PFRDA.
5. Third-party Software: The SI must not use third-party software that isn't commercially available to PFRDA on reasonable terms. All necessary software and hardware must be disclosed to PFRDA and SI should procure all such licenses and software that are required for successful execution of the project, at its own costs.
6. Infringement Remedies: If a deliverable infringes third-party intellectual property rights, the SI will, at its expense, either modify the deliverable to be non-infringing or obtain a license for PFRDA's continued use, at SI’s costs.

xxxvii. **Disputes/Arbitration**

1. Any and all disputes between the Parties arising out of or in connection with this Agreement, or its performance, or touching any aspect thereof shall, so far as possible, be settled amicably among the parties within 30 days after receipt of notice thereof from the party raising the dispute. In case the Parties fail to reach an amicable settlement, any and all disputes between the Parties arising out of or in connection with this Agreement or its performance, or touching any aspect thereof shall be settled by way of arbitration to be conducted under the provisions of the Arbitration and Conciliation Act, 1996, as amended from time to time, by a sole arbitrator to be appointed with the consent of both the parties. Failing any agreement to appoint a sole arbitrator as aforesaid, each party shall appoint one arbitrator, and the two appointed arbitrators shall appoint a third arbitrator, who shall act as the presiding arbitrator. Any further proceedings out of or in relation to such arbitration proceedings, which either party to this agreement may wish to initiate against the other, shall be instituted in courts at New Delhi only.
2. System Integrator shall continue work under the Contract during the arbitration proceedings unless otherwise directed by PFRDA or unless the matter is such that the work cannot possibly be continued until the decision of the arbitrator is obtained.
3. Arbitration proceeding shall be held in Delhi, India, and the language of the arbitration proceedings and that of all documents and communications between the parties shall be in English.

4. Subject to the arbitration clause, only the Courts at New Delhi shall have exclusive jurisdiction to try any disputes arising between the parties, under this agreement or touching any aspect thereof.

xxxviii.**Amendment**

Any amendment to this Agreement shall be made with by mutual written consent of both the Parties.

xxxix. **Miscellaneous**

1. The personnel assigned by System Integrator to perform the Services shall be employees of System Integrator, and under no circumstances shall such personnel be considered employees of PFRDA. The System Integrator shall have the sole responsibility for the supervision and control of the personnel deployed in the Project and for payment of such personnel's compensation, including salary, withholding of income taxes and social security taxes, worker's compensation, employee, and disability benefits and the like and shall be responsible for all obligations of an employer subject to Applicable Law.
2. The System Integrator shall use its best efforts to ensure that sufficient System Integrator personnel are assigned to perform the Services and that such personnel have appropriate qualifications to perform the Services. After discussion with System Integrator, PFRDA shall have the right to require the removal or replacement of any System Integrator personnel performing work under this Agreement based on bona fide reasons. In the event that PFRDA requests that any System Integrator personnel be replaced, the substitution of such personnel shall be accomplished pursuant to a mutually agreed upon schedule.
3. In the event that PFRDA and System Integrator identify any personnel of System Integrator as "Key Personnel", then the System Integrator shall not remove such personnel from the Project without the prior written consent of PFRDA unless such removal is the result of an unavoidable circumstance including but not limited to resignation, termination, medical leave, etc.
4. Each Party shall be responsible for the performance of all its obligations under this Agreement or the SLA as the case may be and shall be liable for the acts and omissions of its employees and agents in connection therewith.

This Agreement shall be with effect from <<dd/mmm/yyyy>>.

In WITNESS WHEREOF the parties hereto have executed this Agreement as of the day and year herein above written.

SIGNED for and on behalf of PFRDA, (PFRDA) By Sh.	SIGNED for and on behalf of System Integrator (SI) By Sh.
Signature_____	Signature _____
Witness_____	Witness_____
Name:	Name:
Place:	Place:
Date:	Date:

xl. RFP Document

<<Published RFP document including corrigendum/Addendum, if any>>

xli. BID Response from SI

<<Bid response from SI will be placed here>>

SCHEDULE I: Implementation Timelines

The total period for the project will be of six (06) years comprising of Twelve (12) months of development and implementation period (Go-live) from the date of the award of the contract, Twelve (12) months of warranty & stabilisation and AMC for Forty-eight (48) months from the date of letter of intent/award.

Milestones	Indicative Key Deliverables/Activities
Letter of intent/award	
Signing of Agreement/Contract	Within 30 days of receiving the letter of intent/award from PFRDA
Requirement Gathering (As-is & To-Be Analysis)	- Understand the existing processes, workflows, Infrastructure etc. - Propose interactive User interfaces with Functionalities for seamless and integrated solution
Research and Design	- User interactions, Use Cases, User Interface Design, Templates
Documentation	Functional Requirement Specification (FRS), Software Design Document (SDD), UI & UX Specifications Document and System Requirement Specification (SRS)
Development – Customization/Configuration/3rd Party Integration	- Source Code & APIs
Deployment	- Setting up of test environment, Installation, Commissioning, Implementation, and security check Manuals

Milestones	Indicative Key Deliverables/Activities
Testing (UAT)	- Certificate for completionof Testing, UAT, Test plans/Test Scripts and - Sample test data
Implementation	- Completion of VAPT, Deployment, Security Audit, Audit Compliance
Training	- User and Technical Documentation, Training, Feedback from Users, Handbook
Go Live	- Certificate of Completion (180 days after Go Live), feedback from PFRDA Employees
Support & Maintenance	- Post Go-LIVE, Twelve (12) months of warranty & stabilisation and AMC for Forty-eight (48) months. - Other integrated solutions version Update and Upgrades

SCHEDULE II: Indicative High Level Functional Requirements for PFRDA-TRACE (PFRDA - Tracking Reporting Analytics & Compliance e-Platform)

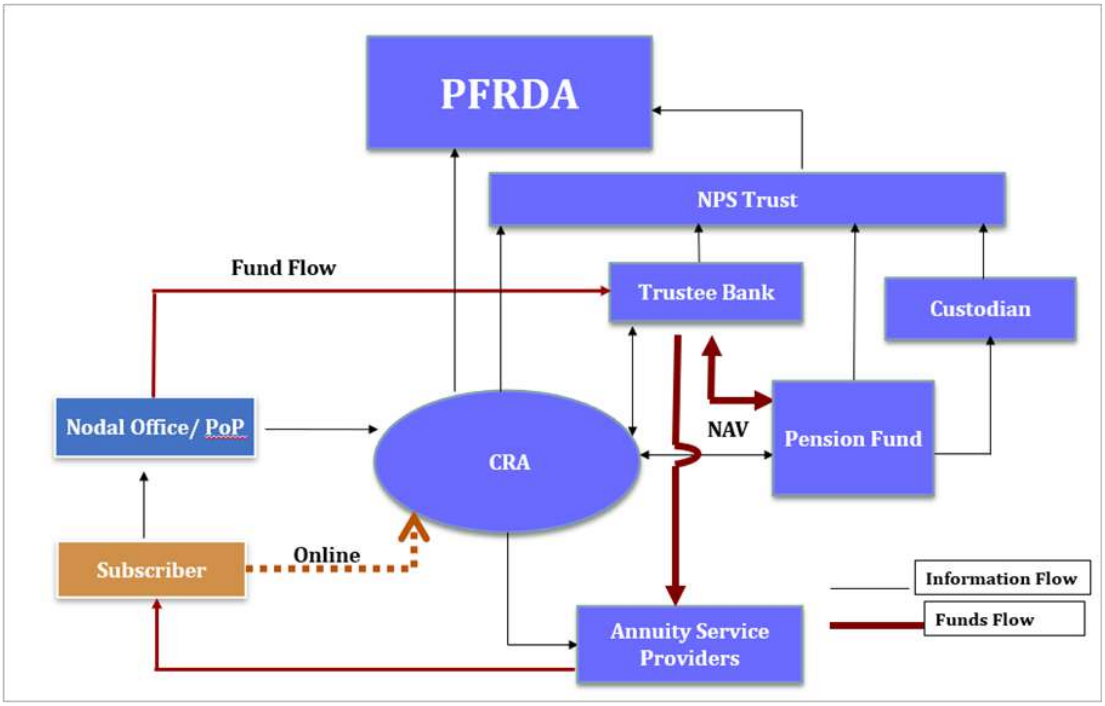
1. PFRDA Digital Compliance Platform module

PFRDA intends to implement a suitable, user-friendly, and robust digital platform to measure and monitor compliance across PFRDA regulated & administered ecosystem effectively and efficiently.

To do this, PFRDA plans to provide to the stakeholders an e-PLATFORM to onboard registered intermediaries and submit the compliance reports which enables PFRDA to perform compliance assessments with a detailed scope and frequency as required under PFRDA regulations which are issued/amended from time to time. PFRDA also intends to use the platform to consolidate and analyse the reports submitted by registered intermediaries.

The proposed e-PLATFORM is designed to offer a self-service interface to Regulated Entities (REs) for the seamless submission of compliances. The portal provides a centralised location for users of intermediaries to access and manage all of their compliance-related information and tasks, including submitting and tracking regulatory filings, managing user access and permissions, and viewing compliance reports. Additionally, it will feature a dedicated interface for PFRDA officials, enabling them to efficiently monitor and track compliances. The platform will also incorporate robust analytics capabilities, including mechanisms for handling exceptions and deviations in compliances submitted by the respective REs . This comprehensive solution aims to streamline the compliance submission process, enhance monitoring capabilities, and facilitate effective analytics for both regulated entities and PFRDA officials.

The e-PLATFORM will facilitate appointed & authorised users from all of these intermediaries to submit the compliance and other reports, as opposed to submitting them via emails, attachments, and physical copies. Here is an overview of NPS architecture.



Key Objectives:

The key objectives of digital transformation of Regulatory and Supervisory activities are as follows:

1. Create an e-PLATFORM for all PFRDA regulated entities.
2. Create a single window with features for regulatory & supervisory activities.
3. The e-PLATFORM to increase collaboration inside PFRDA regulatory & supervisory domain.
4. Increase data Analytics and reporting capability.
5. Information interoperability and Integration with CRA & other systems.
6. Speed up response time through process automation.
7. Monitor & Report non-compliance.
8. Protect subscriber's interest through technology.
9. Optimise quality of supervisory response.
10. Integrate seamlessly with compliance focused supervision.
11. Ease of compliance through digitalization.
12. Implement audit Trail and Traceability.
13. Compliance Workflow and Notifications.
14. Overall technical performance improvement.

Key functions of the proposed e-PLATFORM shall include but not limited to:

1. **Compliance Submission:** The interface for regulated entities will provide the access to submit regulatory cum supervisory reports to PFRDA and REs will be able to view the status of their respective submitted reports. Some of the reports shall include filing forms, details of payment of fees, attachments, various compliances, and other related documents.
2. **Compliance monitoring & supervision:** the system shall facilitate to view compliance reports submitted by the intermediaries, check compliance status and progress towards meeting regulatory requirements and perform analytics.
3. **User access and permission management:** The system shall facilitate user access as per the roles & privileges defined.
    a. Add/moderate user group (CRA , Pension Funds, PoPs, etc)–
    b. Add/moderate user roles (Admin of the user group add , assign, remove user groups)–
    c. Add/moderate user privileges (assign & manage user roles from PFRDA side in the super admin c-panel)-
    d. Dynamically assign user group/role to specific workflow, report, data structure, RPA flows which are already designed.
4. **Automated & Dynamic Workflows and alerts:** the e-PLATFORM shall include automated workflows and alerts to assist in verification of compliance tasks and deadlines. Workflows in the e-PLATFORM should be configurable and non-restrictive from technology, business, integration, or other avenues. Example – maker checker model should be implemented where a report is getting submitted and likewise. The system should also facilitate PFRDA to create a new report & seek the same from user group in some existing or new workflow. Adding any entity in the existing workflow should be felicitated by the system without any development effort. Relevant workflow reporting & associated all other components should be automatically part of the user journey for the newly added entity after the entity is onboarded.
5. **Document Management:** the portal must allow users to manage all documents including submitted reports. Maintain a repository of documents via automated meta data tags; with the ability to navigate to the documents via standard filters & search.
6. **Analytics & Dashboards:** The e-PLATFORM should be equipped with analytics dashboards & infographics relevant for the user for better user experience & platform intuitiveness. The users should be able to slice & dice from the available source of data, according to established data cohesion or logic.
7. **Integration & Validation of DSC/e-Sign** : The platform shall facilitate digitally sign & e-sign on the submitted reports wherever applicable. The DSC/e-signatures should be validated by the system.
8. **Rule based exception & deviation handling/highlighting:** PFRDA should be able to create a framework which will moderate a rule engine to monitor & highlight according to pre-set logic, scenarios in case-to-case basis.
9. **BI tools slicing & dicing capability:** The Business Intelligence tool should empower users with robust slicing and dicing capabilities, allowing dynamic exploration of

available data and reports. The SI should ensure that users should seamlessly use this feature to facilitate insightful analysis and informed decision-making.

10. **Collaboration platform**: A key objective of the platform for the Supervisory Department is to perform their tasks in more efficient and automated manner which would include processing of data & information, two-way communication among PFRDA officials as well as with the intermediaries.
11. **Reporting – template driven & query based:** The system should be capable of having a reporting mechanism which would prefetch reports on predeveloped templates & would also be capable of creating new reports from user driven GUI.

a) Regulatory Activities

Following are the indicative broad process steps performed by Regulation Departments in PFRDA which needs to be incorporated in the system.

Sr No	Processes
1	Onboarding process of intermediaries
2	Annual Compliance for confirming eligibility for all registered intermediaries
3	Collection of Payment details of Regulatory Fees as applicable
4	Submission of information for PFRDA approval in case of change in constitution of the intermediaries
5	Submission of information in case of change in Name/Director/Independent Director/Key Personnel/Shareholding pattern and Compliance Officer
6	Submission of pending legal cases at the time of selection or thereafter by intermediaries to regulation department.
7	Disclosure of additional information to PFRDA by the intermediary as required.

b) Supervisory Activities

Following are the indicative broad process steps performed by Supervision Departments in PFRDA.

S. No	Reporting Entity	Role of the Department
1	Supervision - Annuity Service Provider (ASPs)	- The responsibility and process to be followed for various activities for supervision of Annuity Service Provides includes reviewing the performance of ASP for their adhering to the regulation and terms of empanelment for disposing off the annuity purchase request and integration of ASP with CRA, providing comments to regulation department on Framing/Reviewing/Modifying Exit and Withdrawal Regulations related to Annuity and Annuity service providers
2	Supervision - Central Recordkeeping Agency (CRA)	- The Supervision CRA department is to ensure that the Central Recordkeeping Agencies (CRAs) are carrying out their roles and responsibilities as per the rules, regulations and guidelines issued by PFRDA. Automated Monitoring of Compliance status of all business/operational and technical SLAs with CRA is monitored on regular intervals. Periodic review of MIS submitted by CRA at regular intervals. Based on these MIS's the various parameters defined by PFRDA are tracked to measure the performance of the CRAs.
3	Supervision - NPS Trust	- NPS Trust holds the subscriber's funds in its name while subscriber is the beneficial owner. The responsibilities of the department include monitoring the performance of NPS Trust as per their roles, responsibilities, and various activities. - Monitoring performance of NPS Trust as per role and responsibility of NPS Trust prescribed in NPS Trust Regulations to improve its efficiency, monitoring resolution of Grievances escalated to NPS trust and scrutinising the exception/deviation report of Compliance/Audit/Inspection w.r.t. intermediaries forwarded by NPS Trust (CRA/TB/ASPs/Grievances)

S. No	Reporting Entity	Role of the Department
4	Supervision - Trustee Bank	- The responsibilities of Supervision - Trustee Bank includes the perusal and examination of MIS, performance reports, Audit reports, examination of balances, Inspections, and development of functionalities, if any in coordination with CRA for the benefit of subscribers. Reports of Trustee Banks are analysed by NPS Trust. They submit their analysis with recommendations to PFRDA. PFRDA examines further and directs Trustee Bank, CRA & NPS Trust to take corrective actions and also monitors the progress on regular basis with respect to Quarterly Concurrent Audit Report, Annual Audit Report, Annual Statutory Audit Report, Half yearly Cyber Security Report and Pool Reconciliation.
5	Supervision - Custodian of securities	- The Supervision Custodian Department has the role to monitor and supervise the activities undertaken by the Custodian to ensure smooth discharge of the functions by the Custodian. - Broad responsibilities of the department include, Evaluating the reports like monthly reports w.r.t AUM V/SAUC, quarterly Internal Audit Reports submitted by NPS Trust for the Custodian to PFRDA on periodic basis. Other supervisory functions like reconciliation of holdings with the Pension Funds by the Custodian, review of internal audit reports & compliance of the same, compliance of breaches, etc
6	Supervision - Pension Funds	- To ensure such efficient discharge of functions and duties as prescribed under the Regulations, PF-Supervision Department is expected to undertake offsite as well as onsite monitoring & supervision of PFs which includes the review of the Periodicals, on site visits, inspection. - Broad responsibilities of the department include Periodic Review of performance of Pension Funds through review of periodic Reports/MIS returns submitted by PFs and NPS, Ensuring Compliance by the Pension Funds on certain submissions as prescribed by PFRDA from time to time, Analysis of Quarterly supervisory certificate on investment/sectoral limits as per the investment guidelines issued by PFRDA and MIS on quarterly group exposure in group companies

S. No	Reporting Entity	Role of the Department
7	Supervision - Central Government and State Government	- The endeavour of the Supervision-CG/SG/CABs/SABs department is to undertake supervision and monitoring of the NPS related activities under the Government Sector viz. Central Government Ministries/departments and State Governments. - Broad responsibilities of the department include Analysis of various reports submitted by CRA to ascertain the performance of Govt. Sector Nodal office. Monitoring of the performance of Central Government Ministries/departments and State Governments including Central and State Autonomous Bodies in implementation of NPS.

c) Policy Research and Market Watch

Policy Research and Market Watch Department conducts research on various financial aspects and analyses various reports for NPS related data. It is also responsible for preparation of statistical handbook based on compilation of data.

d) Promotion and Development

Promotion and Development Department of PFRDA conducts promotion and development activities related to NPS and APY.

2. Implementing the Digital Platform for Regulatory Business Process

a) Onboarding of Stakeholders

1. User Types for Intermediaries

User Types	Primary Role
Maker	- As a role type, Makers are operators of the digital platform and responsible for entering data, information, and uploading the required reports to the digital platform in a timely manner. - However, all the information that they will enter, will not be submitted to the platform, but only saved for review by the Checkers. - The makers may continue to edit or upload more information until the Checker reviews and approves the same.
Checker	- The Checkers have the dual role of reviewing and approving the submissions made by the maker.

User Types	Primary Role
	- Checkers will be notified of all the changes the Makers make and will be responsible for verifying the accuracy and completeness of the report and will have the capability to approve the report in the platform itself and send the report to PFRDA. - Checkers may choose to approve directly, or edit before approval, after which the information shall be submitted to PFRDA. - Many intermediaries may only have one user to manage the platform, who could have both the roles as defined by PFRDA admin.
Admin	Admin is responsible for managing access control to the digital platform and for assigning different roles to the relevant functional users at the intermediary level.
Key Considerations	- The User Type (Maker and Checker) must be applied to all users via the RBAC (Role Based Access Control) interface and also via the IAC (Individual Access Control) interface. - The Intermediary admin should be able to view key user roles as per the intermediary they are administering, and their privileges should be pre-defined as per respective PFRDA Departmental Admin. However, these could be altered using the Intermediary Admin User Interface. - Any user with intermediary will have to reset their password and authenticate their Phone or Corporate Email IDs at a configurable interval. And the system should be able to alert, prompt and enforce the same. More on this discussed in the Application Security section in Technical Architecture Document.

2. User Types for PFRDA

User Types	Primary Role
Super Admin	A Super Admin is the highest level of administrator and has the most extensive permissions and access to all features of the platform. - Access and modify the core settings and configurations of the platform. This can include everything from setting up new user roles and permissions to configuring system-wide settings and preferences. - Create, edit, and delete user accounts and assign them to different roles, types. They can also manage user permissions and access levels within the platform. - Access and manage all content and data on the platform, including creating, editing, and deleting content as well as controlling access to it. - The super admin should be able to define new roles and grant privileges for the same.

User Types	Primary Role
	- To create admin as per the role & access privileges.
Admin	The admin role at PFRDA will have the functionality of viewing, creating, editing, and deleting new departments, roles, users as and when required. - The Self-service theme is applicable for PFRDA Admin users who should be able to access and configure the portal for all stakeholders. - Onboarding existing intermediaries and giving the required access to their authorised personnel. - View system logs by user, by department, storage space utilised, last logins, etc. - Define notification triggers, texts, and channels for stakeholders inside and outside of PFRDA.
Department Roles	All departments inside PFRDA will have their own role hierarchy mapped to the User Roles and Users. Departments will have their admin roles as well, whose privilege will be limited to manage Department roles and users. SI to work with PFRDA departments to define these users' roles further with access privileges for each. Not all roles are applicable to all departments.
Appointed System Auditor	- Monitor the performance of the platform and its underlying systems, as well as managing security settings and monitoring for potential threats. This role could be assigned to an external party appointed by PFRDA for audit purposes.

3. <u>Standard Profile View for all Intermediaries</u>

Profile & Workspace Interface	All intermediaries shall have a Profile page of their own that will display all the information shared with PFRDA thus far. The profile shall capture a summary. Including the following functions but not limited to – - Current Compliance Status - Company Information - Directors Info - Payments History/Records - Legal Information & Disclosures. - Compliance Requirements - Self-Declaration

- PFRDA Registration Information such as registration date, registration code, validity of the registration, renewal date, details of the renewal fee, details of annual fee, etc.
- Users and Roles (with status of Makers, Checkers and Admins)
- Reports & Dashboards (Preferably the landing page)
- Alerts & Notifications
- Any other Settings required to manage their profile.
- Audit Logs of each of the above

4. Compliance Fee and Other Payment

Payment details	- All intermediaries will be able to view compliance & renewal fees they are required to pay on a regular and recurring basis. - These payments can be on a monthly, quarterly, or annual basis – based on frequency setup & the amount by PFRDA via regulations & guidelines. - Some intermediaries calculate their own fee and submit evidence of fee calculation which will be validated by the system if the data is available. - The provision of upload of details in respect of fees such as application fee and registration fee paid by these intermediaries at the time of seeking registration and after registration respectively should be made available. - Recording payment details: The amount could be paid outside of PFRDA platform, like NEFT or RTGS. There should be a provision to record the transaction details; and also provide supporting evidence of the payment made. - Invoice generation: The platform should generate invoices for the regulatory fee payments, which can be viewed, downloaded, and printed by the user. For payments made online, the invoices & receipts are to be provided automatically. For any payments made via bank transfer, the invoices are generated by the F&A department of PFRDA at the central level. It may be available to users post validation. - Payment history: The platform should keep a record of all regulatory fee payments made by the organisation, including the date, amount, and payment status. - Automatic reminders: The platform should send automatic reminders to the user to pay their regulatory fee before the due date. PFRDA system shall notify CRA, TB, ASPs, PFs, Custodians to pay quarterly regulatory fee. - Notification should go out to the compliance officers. - The notification should go out as emails, SMS, and as visible alerts within the Regulatory system. - The notifications should go out ahead of time, mentioning the amount/clause related to the calculation of amount and the due date and grace period. - An exception in automatic reminders for CRA, TB, and ASPs because neither amount is fixed nor there is a concept of grace period for payment of fee. These notifications need to be carefully designed. - Audit trail: The platform should maintain an audit trail of all actions taken by the user on the platform, so that the organisation can track their actions and monitor compliance with regulatory requirements. Including failed payments.
Payment of Penalties	- The Enforcement department of PFRDA, in consultation with the Regulatory and Supervisory Department, may levy fines and penalties on intermediaries. - All intermediaries should be able to view if any fines or penalties are levied on them. - A notification should be sent out in case of any penalties. - Receipt generation: The platform should generate receipts for the fines and penalties, which can be viewed, downloaded, and printed by the user.

	- Payment history: The platform should keep a record of all regulatory fee payments made by the organisation, including the date, amount, and payment status.
Any Other fees	- PFRDA team could solicit any other fee on ad hoc or regular basis. The provision for the same should be made.
Fee Process	CRA - Annual Fee - Quarterly - Calculated by intermediary. TB - Annual Fee - Quarterly - Calculated by intermediary. ASP - Renewal Fee - Quinquennial - Fixed As the Annual fees paid by CRA and TB are calculated at the end of intermediaries and verified at PFRDA, provisions for the upload of relevant documents by intermediaries and verification by PFRDA may be made available.

b) RegTech Module

1. For CRA, TB, ASPs

Functional Area	Overview
Company Information	This will include all information about the company such as: - Name - Location - Contact Details - Single Point of Contact (i.e. Current Compliance officer) - Company Registration Documents and mandatory disclosures. - Previous Compliance Officers, their tenure, and their roles. - Escalation Matrix, as defined by the intermediary. - Other standard company information as defined by PFRDA team.
Annual Compliance and Eligibility.	- CRA, TB, ASPs should be able to view annual compliance requirements and should be able to submit relevant documents to stay compliant. - Exit Management Plan and Compliance Certificate are shared by CRAs Annually. - PFRDA team should be able to create a compliance request for an individual intermediary, intermediary type, or all intermediaries at once clearly defining the requirements, documents required and Date of submission of compliance. This could be a recurring compliance requirement or an ad hoc one. - In case of any objection/clarification send the request back for review any number of times by giving comments. Should be able to send manual reminders, apart from the automated ones. - Rule engine-based compliance validations: The system should have the capability to validate the compliance responses.

Functional Area	Overview
	- Initiate Ad Hoc compliance requirements: Intermediaries should be able to view additional compliance requirements, if PFRDA asks for the same on an ad hoc basis. The system should show the documents required, and the last date for submitting proofs of compliance. - Notifications: Users of CRA, TB, ASPs, should be notified via email and SMS as soon as these ad hoc compliance requests are made. The notifications should include the last date for submission and the documents required. - Submission of response and documents: Users of the intermediary should be able to respond to the ad hoc compliance requests by writing a response and uploading the required documents. This should follow the Maker-Checker default workflow and be submitted for verification. - Annual compliance needs: Apart from ad hoc compliance needs, there should be annual compliance. The system should send out notifications ahead of time, and also during the grace period. - Compliance history and logs: The system should provide a way for the user to view all previous compliance requests, their status, and logs of status & all documentary evidence of the same.
Self-Declaration and Regular Updates	Regular submission of information in case of change in Name/Director/Independent Director/Key Personnel/Shareholding pattern and Compliance Officer. - The platform should provide a way for users to submit any changes in the organisation's name, directors, independent directors, key personnel, shareholding pattern, and compliance officer. For any change in the above, users should be able to make edits on the screen. A supporting, digitally signed document must be uploaded and submitted to PFRDA. - Validation: The platform should validate the form submissions for completeness and accuracy. - Document upload: The platform should provide a way for users to upload supporting documents, such as copies of official documents, in support of the form submissions. - Approval workflows: The platform should provide a way for users to submit forms for approval and track the status of their approvals. Like everything else on the Platform, this will also follow the Maker-Checker Workflow, including the notification triggers and Digital Signature by the Checker. - Notifications: The platform should send notifications to the user as required .

Functional Area	Overview
	- Audit trail: The platform should maintain an audit trail of all actions taken by the user on the platform, so that the organisation can track their actions and monitor compliance with regulatory requirements. This should show logs of change with the change being done, by which user, date, and time stamps.
Legal Disclosures (Applicable for all Intermediaries)	- Ability to capture legal information, including but not limited to adding details of pending legal cases at the time of selection. This must include soliciting disclosure of all legal information that may impact the selection. - Compliance with legal and regulatory requirements: to ensure that the platform adheres to any relevant legal and regulatory requirements regarding the collection, storage, and use of legal information. - Inform users of how their legal information will be used, stored, and protected. And take consent before storing information. - Data minimization: work with business to collect only the minimum amount of legal information required to fulfil the platform's purpose. - It'll include uploading documents (all extension types, with no size limits), hyperlinks, and other formats of soliciting information.
Digital Documents and Signature Verification	- Digital document handling and signature verification, with the ability to upload and store documents.
Download Reports	- All documents must be stored in a secured manner. - Every time PFRDA team downloads the document uploaded by the intermediary, it should ask the user the file extension one wants to download in, for example PDF, XLS, CSV, WORD, etc. The source file format should be highlighted.
Maintain Historical Details	Ability to store and view historical details of all records, when were they updated and by which user.

Functional Area	Overview
Reports and Queries	Dashboard for generating various reports and queries, such as - List of all intermediaries filtered by - intermediary type, - Compliant and non-compliant - Renewing soon or date of expiry or date of registration, - details of annual fee or renewal fee submitted, - Details of compliance officer including the history of changes - Other similar reports
Two Way Communication	In cases where the Department wants to send out a message, circular, a notification, request for additional documentation, that can be initiated from the relevant department within PFRDA. This communication could be directed to either all intermediaries, an intermediary type, or a named intermediary. PFRDA department may also want to share caution letters, warnings, and directions to intermediaries, which should be private and visible only to that intermediary in question. This will trigger notification on the portal and will be visible to their users when they login to PFRDA platform. And will also go out as an email/SMS notification, with a secure hyperlink to the notification. In case the intermediary seeks some special approvals from PFRDA, the portal should be able to cater to those requirements and should notify the relevant department for the same.

Brief Activities pertaining to the CRA, TB and ASPs

- Annual Compliance for confirming eligibility for CRA, TB & ASP
- Details of payment of Regulatory Fees on a quarterly basis for Trustee Bank and CRA, with a capability to notify and get confirmation from the Finance and Accounts department for the same.
- For CRA, TB & ASP: Submission of information in case of change in Name/Director/Independent Director/Key Personnel/Shareholding pattern and Compliance Officer
- For CRA : Details of pending legal cases at the time of selection and disclosure of information in the capacity of CRA regarding legal cases.
- Process should be designed to self-onboard them onto the e platform.
- Functionality to search for historical details of group companies and directors of companies should also be provided.

- For CRA, TB & ASP : Dashboard for generation of various kinds of reports/queries as per the requirement of department like date of expiry or date of registration, renewal, details of annual fee or renewal fee submitted and details of compliance officer including the history of changes.

2. <u>For PF (Pension Funds), Custodian and NPS Trust</u>

Company Information	This will include all information about the company such as - Name - Location - Contact Details - Single Point of Contact (i.e. Current Compliance officer) - Other Key Personnels details and contact details. - Company Registration Documents and mandatory disclosures. - Previous Compliance Officers, their tenure, and their roles. - Other standard company information as defined by PFRDA team.
Alerts for Fees and Compliance	- System Alerts: The system should be able to generate alerts for the timelines of submission of annual fee and compliance reports. - The user should be given the flexibility to set up alerts on their own on the system to set and manage timelines for the submission of annual fee and compliance reports. - Reminders: The system should send reminders to the intermediaries about the upcoming deadlines for the submission of annual fee and compliance reports over emails/SMS. - Smart Alerts: The system should stop alerting the user once all documents and fees are paid for the current requirements. System should notify the users once the fee and compliance resorts are accepted or rejected.
Annual compliance for PFs, and Custodians.	- Pension Funds should be able to view annual compliance requirements and should be able to submit relevant documents to stay compliant. - PFRDA team should be able to create a compliance request for an individual intermediary, intermediary type, or all intermediaries at once clearly defining the requirements, documents required and Date of submission of compliance. This could be a recurring compliance requirement or an ad hoc one. - send requests for review any number of times by giving comments. Should be able to send manual reminders, apart from the automated ones. - Rule engine-based compliance validations: The system should have the capability to validate the compliance responses. Initiate Ad Hoc compliance requirements: PF and Custodians should be able to view additional compliance requirements, if PFRDA asks for the

	same on an ad hoc basis. The system should show the documents required, and the last date for submitting proofs of compliance. - Notifications: Users of PFs, and Custodians, should be notified via email as soon as these ad hoc compliance requests are made. The notifications should include the last date for submission and the documents required. - Submission of response and documents: Users of the PFs and Custodians should be able to respond to the ad hoc compliance requests by writing a response and uploading the required documents. This should follow the Maker-Checker default workflow and be submitted for verification. - Annual compliance needs: Apart from ad hoc compliance needs, there should be annual compliance. The system should send out notifications ahead of time, and also during the grace period. - Compliance history and logs: The system should provide a way for the user to view all previous compliance requests, their status, and logs of status & all documentary evidence of the same.
Approvals in case of change in the constitution	- In case of amendment in constitution, such as - Change in company from Private to Public or Public to Private. - Shareholding Pattern - Change of Directors - IPOs and FPOs - Any amendments in Pension Fund Regulatory & Development Authority Act PFRDA team should be able to solicit additional documentation from intermediaries. These requirements will follow the same workflow as defined above in the Compliance section. - Any further requirement on account of amendments in PFRDA Act, Regulations, Guidelines, or any other circular issued by PFRDA team should be able to solicit additional documentation from intermediaries. These requirements will follow the same workflow as defined above in the Compliance section. - Automated compliance checks: The system should have the capability to perform compliance responses to reduce the time taken for the approval process. Only highlight the pending documents waiting to be reviewed. - Compliance requirements: PFs and Custodians should be able to view compliance requirements, if PFRDA asks for the same. The system should show the documents required, and the last date for submitting proofs of compliance. - Notifications: Makers and Checkers of PFs, Custodians, should be notified via email/SMS as soon as these requests are made. The

	notifications should include the last date for submission and the documents required. - Submission of response and documents: Users of the PFs and Custodians should be able to respond to the requests by writing a response and uploading the required documents. This should follow the Maker-Checker default workflow and be submitted for verification. - Compliance history and logs: The system should provide a way for the user to view all previous compliance requests, their status, and logs of statuses & all documentary evidence of the same.
Self-Declaration and Regular Updates.	Regular submission of information in case of change in Name/Director/Independent Director/Key Personnel/Shareholding pattern and Compliance Officer. - Custodians must declare Any change in registration status, any penal action taken by any Authority, or any material change in financials. - Form creation and submission: The platform should provide a way for users to create and submit forms related to changes in the organisation's name, director, independent director, key personnel, shareholding pattern, and compliance officer. - Validation: The platform should validate the form submissions for completeness and accuracy - Document upload: The platform should provide a way for users to upload supporting documents, such as copies of official documents, in support of the form submissions. - Approval workflows: The platform should provide a way for users to submit forms for approval and track the status of their approvals. Like everything else on the Platform, this will also follow the Maker-Checker Workflow, including the notification triggers and Digital Signature by the Checker. - Notifications: The platform should send notifications to the users as required . - Audit trail: The platform should maintain an audit trail of all actions taken by the user on the platform, so that the organisation can track their actions and monitor compliance with regulatory requirements. This should show logs of change with the change being done, by which user, date, and time stamps.
Auto Alerts & Notifications	- Enabling Alerts via email, SMS (if applicable) and other channels to PFs, Custodians and NPS Trust for timelines of Submission of Annual Fee and Compliance reports . - Alerts to admin for any delays, failures, and success of payments. System notification and also via other standard channels.

	- PFRDA should be able to set notification preferences and edit the notification content via PFRDA Admin interface.
Statement of assets under management for payment of Annual Fee (on Quarterly basis)	- PFs must be provided with an interface to upload and declare statements of assets under management for payment of Annual Fee to be paid on quarterly basis. - Custodians must be provided with an interface to upload reports on AUC submitted by PFMs vs. AUC reported by Custodian to identify any anomalies and verification of regulatory compliance fees submitted by Custodian on an annual basis. - A covering letter on the letter head must be accompanied with the above details.
Digital Documents and Signature Verification	- Digital document handling and signature verification, with the ability to upload and store documents online and ensure that the documents are verified by the authorised person. - All documents must be digitally signed.
Reports download	- All documents must be stored in a secured manner. - Every time PFRDA team downloads the document uploaded by the intermediary, it should ask the user the file extension one wants to download in, for example PDF, XLS, CSV, WORD, etc. The source file format should be highlighted.
Two Way Communication	In cases where PFRDA Department wants to send out a message, circular, a notification, request for additional documentation, that can be initiated from the relevant department within PFRDA. This communication could be directed to either all, some or named intermediary, users. PFRDA department may also want to share caution letters, warnings, and directions to PFs, Custodian or NPS Trust, which should be private and visible only to that user it is intended for. This will trigger notification on the portal and will be visible to their users when they login to PFRDA platform. And will also go out as an email notification, with a secure hyperlink to the notification. In case the intermediary seeks some special approvals from PFRDA, the portal should be able to cater to those requirements and should notify the relevant department for the same.
Requirements for NPS Trust	
Submission of	- Process of submission of particulars of interest by trustees

documents for Trustees	- Ability to submit resignation/completion of tenure of trustees. And maintain a history of Trustees.
Dashboard	Dashboard for generation of various kinds of reports/queries as per the requirement of the department like date of appointment/extension/expiry or tenure of trustees, the appointment of chairman on board of NPS trust, details of nomination by CG/SG. The system should alert if Trustees are getting retired. This alert should be at least 6 months ahead of time. Ability to select date range and other standard filters are implicit in a reporting view. Ability to create new reports by dragging and dropping metrics and curating a new report. Ability to save a report and create a shortcut to view the curated report in future. Ability to receive alerts & notifications if anomalies are found in the report from the expected standards.

Brief of activities pertaining to PFs, Custodian and NPS Trust

Pension Funds

- Details of payment of fees as mandated by PFRDA i.e., quarterly. Statement of assets under management for payment of Annual Fee (on Quarterly basis)
- Annual compliance for confirming eligibility.
- Submission of information regarding change in shareholding pattern/independent director/ownership/controlling interest of sponsor/management/key personnel including compliance officer
- Enabling Alerts to PF for timelines of Submission of Annual Fee and Compliance reports
- Shareholding pattern, undertaking along with a certified copy of resolution passed by the Board of Directors confirming the compliance of “Indian owned and controlled” under Guidelines on aggregate holding of equity shares by a foreign company in PF i.e., half yearly (2nd and 4th quarter)
- Details of Registered PFs along with details of Key personnel including Directors/Independent Directors of PFs and Sponsors.
- Reports on AUM received from NPST vs. AUM reported by PFs to identify any anomalies and verification of regulatory compliance fees submitted by PFs.

Custodian

- Details of payment of annual fee as mandated by PFRDA along with statement of assets under management on quarterly basis.
- Annual compliance for confirming eligibility.
- Enabling Alerts to Custodian for timelines of Submission of Annual Fee and Compliance reports
- Compliance reporting for Change in registration status or any penal action taken by any authority or material change in financials.
- Reports on AUC received from NPST vs. AUC reported by Custodian to identify any anomalies and verification of regulatory compliance fees submitted by Custodian.

NPS Trust

- Process of submission of Annual Report w.r.t beneficial/material interests of the Trustee in any other company of institution or body corporate i.e., frequency would be annual and when the trustee initially appointed.
- Details of resignation/completion of tenure for trustees.
- Dashboard for generation of various kinds of reports/queries as per the requirement of department like date of appointment/extension/expiry of tenure of Chairman & trustees, details of nomination by CG/SG.
- Compliance filings pertaining to PFs, Custodian, Trustee Bank and for exit related matters pertaining to CRA's for respective PFRDA supervision or regulation department.

3. <u>For PoP (Point of Presence)</u>

Profile & Workspace Interface	PoPs will have a Profile page of their own that will display all the information shared with PFRDA thus far. The profile shall capture a summary. Including the following functions - Company Information - Directors Info - Escalation matrix - Payments of Fees & History - Legal Information & Disclosures. - Compliance Requirements - Self-Declaration - Users (Makers, Checkers and Admins) - Reports & Dashboard (preferably the landing page) - Alerts & Notifications - Or any other Settings required to manage their profile. - Change Logs of each of the above

Payment details	- PoPs will be able to view compliance fees they are required to pay on an annual (as per PoP Regulation, it is to be paid once in 5 years,) and recurring basis. - These payments can be on a monthly, quarterly, or annual basis, and PFRDA admin should be able to define the interval. - The fee will be defined by PFRDA Admin for all intermediaries and may differ with each intermediary type. - There should be a provision to record the transaction details; and also provide supporting evidence of the payment made. - Payment history: The platform should keep a record of all regulatory fee payments made by the organisation, including the date, amount, and payment proof /record. - Automatic reminders: The platform should send automatic reminders to the user to pay their regulatory fee before the due date. - Audit trail: The platform should maintain an audit trail of all actions taken by the user on the platform, so that the organisation can track their actions and monitor compliance with regulatory requirements. Including failed payments. - Document upload feature to be made available. Esp. at the time of renewal.
Annual Compliance for confirming eligibility	- PFRDA team should be able to create a compliance request for an individual intermediary, intermediary type, or all intermediaries at once clearly defining the requirements, documents required and Date of submission of compliance. This could be a recurring compliance requirement or an ad hoc one. - PFRDA should be able to send the request back for review any number of times by giving comments. Should be able to send manual reminders, apart from the automated ones. - Ability to send Forms along with doc upload should be provided. - Ad hoc compliance requirements: Intermediaries should be able to view additional compliance requirements, if PFRDA asks for the same on an ad hoc basis. The system should show the documents required, and the last date for submitting proofs of compliance. - Notifications: Makers and Checkers of POPs should be notified via email and SMS as soon as these ad hoc compliance requests are made. The notifications should include the last date for submission and the documents required. - Submission of response and documents: Users of the intermediary should be able to respond to the ad hoc compliance requests by writing a response and uploading the required documents. This should follow the Maker-Checker default workflow and be submitted for verification.

	- Annual compliance needs: Apart from ad hoc compliance needs, there should be annual compliance needs that will have a rhythmic approach to approval. The system should send out notifications ahead of time, and also during the grace period. - Compliance history and logs: The system should provide a way for the user to view all previous compliance requests, their status, and logs of statuses & all documentary evidence of the same.
Approvals in case of change in the constitution	- In case of amendment in constitution, such as - Change in company from Private to Public or Public to Private. - Shareholding Pattern - Change of Directors - IPOs and NFOs - Any amendments in Pension Fund Regulatory & Development Authority Act - Should be able to send manual reminders, apart from the automated ones. - Compliance requirements: PoPs, CABs, SABs, should be able to view pending approvals, if PFRDA asks for the same. The system should show the documents required, and the last date for submitting proofs. - Notifications: Makers and Checkers should be notified via email/SMS as soon as these requests are made. The notifications should include the last date for submission and the documents required. - Submission of response and documents: Users should be able to respond to the requests by writing a response and uploading the required documents. This should follow the Maker-Checker default workflow and be submitted for verification. - History and logs: The system should provide a way for the user to view all previous compliance requests, their status, and logs of statuses & all documentary evidence of the same.
Digital Documents and Signature Verification	- Digital document handling and signature verification, with the ability to upload and store documents online and ensure that the documents are verified by the authorised person. -
Report downloads	- All documents must be stored in a secured manner. - Every time PFRDA team downloads the document uploaded by the intermediary, it should ask the user the file extension one wants to download in, for example PDF, XLS, CSV, WORD, etc. The source file format should be highlighted.

Regular Information Update and Submission	Regular submission of information in case of change in Name/Director/Independent Director/Key Personnel/Shareholding pattern and Compliance Officer. - Form creation and submission - Standard changes should be solicited from existing pages, for example, changes in the organisation's name, director, independent director, key personnel, shareholding pattern, and compliance officer, designated director, principal officer. Once the users update the information, the same should be supported by documentary evidence. - Validation: The platform should validate the form submissions for completeness and accuracy - Document upload: The platform should provide a way for users to upload supporting documents, such as copies of official documents, in support of the form submissions. - Approval workflows: The platform should provide a way for users to submit forms for approval and track the status of their approvals. Like everything else on the Platform, this will also follow the Maker-Checker Workflow, including the notification triggers and Digital Signature by the Checker. - Notifications: The platform should send notifications to the users - Audit trail: The platform should maintain an audit trail of all actions taken by the user on the platform, so that the organisation can track their actions and monitor compliance with regulatory requirements. This should show logs of change with the change being done, by which user, date, and time stamps. - In case the due date of security is approaching, reminder emails, notification may be sent to the intermediary.
Dashboard for the Intermediary	The users of the intermediaries should be shown insights on their performance, compliance status and other information that are actionable. These data points would include but not limited to - Compliance status - Subscriber count, pulled from all CRAs. - Subscriber demographics data - Grievance data form CGMS of all CRAs to be compiled for analysis of grievances entity-wise, grievance category-wise. This can be hyperlinked to the CGMS portal for users to act. - Pending Exits - Pending Compliance and Reports, with due date - Notifications & Alerts

Dashboards for PFRDA Team	PFRDA team shall require a reporting dashboard that displays reports for PoPs, PoP SEs, CABs, and SABs. - Security Deposit Report - Expiration Reports: A dashboard displaying the expiration date of registration for all stakeholders. - Renewal Report: A report showing the number of renewals due and those that have been completed. Along with the amount collected. - Compliance Dashboard: Annual compliance certificate - Payment Report: A report displaying the details of annual fee or renewal fee payments made by stakeholders. - Compliance Officer Report: A report displaying the information of compliance officers, including a history of changes. - Footprint Report: A report providing details of associated Point of Presence Sub Entities (PoP-SEs) for each stakeholder. - Waivers Report: A report displaying information on any waivers granted to stakeholders. These reports are only indicative and shall have more similar reporting views. All reports should have the ability to - Sort, filter and search data on dimensions and metrics. - Export reports in excels, CSV, via email triggers to keep a log of who downloaded the reports. - Integrate other data visualisation platforms via standard products in the market. PFRDA team, including business users, should be able to generate new reports by defining the metrics on their own, visualise a sample report and generate the report. - Workflow for submission of reports may be made generic and may be decided internally based on existing resources at various levels in the department and not purely based on designation.

Regulation Reports to be submitted by PoPs.

Report	Frequency
Annual Compliance Certificate	Annual
Certificate for Payment of Renewal Fee along with CA Certificate	QUINQUENNIAL
Change in the constitution/compliance officer/designated director/principal officer	Ad-hoc

4. For Retirement advisors

Onboarding & Fee Payment details update	- Existing individual & non individual RAs would be onboarded in the system. - Document and image upload: The RAs should be able to upload documents in the prescribed format as part of the onboarding process. (Digital Sign and E-Sign verified, if required) - PAN validation facility may be made available. - Incomplete application saving: The system should allow RAs to save incomplete applications and allow them to resume application submission at a later stage. - Payment details upload: The system should have facility to record payment details as made. The web form with evidence upload should be facilitated for recording payment details. - Approval and Rejection process: PFRDA team should have the capability to approve or reject the onboarding process and notify the RAs accordingly. The team could also request additional information and documents. PFRDA team should have the ability to put application on hold. - Allow PFRDA team to Pause for auto signups, for Individual RAs, Entity RAs, or both.
Profile & Workspace Interface	RAs, like other stakeholders, should have a Profile page of their own that will display all the information shared with PFRDA thus far. And will also have a workspace to interface with PFRDA. Including the following functions - Details of their Compliance Officer - Company Information - Legal Information & Disclosures. - Compliance Requirements - Payments - Self-Declaration - Reports - Alerts & Notifications - Other Settings - Logs of changes each of the above
Security Deposit and NISM Certificate details	- RAs should be able to view the status of security deposit and validity of NISM certificate. - Details of security deposit of Performance Security or Fixed Deposit. RAs should be able to upload the details, with original copies. - If the deposit is not made, the same should be prompted from the logged in user. And should also be notified via email and SMS at appropriate frequency as defined by PFRDA team.

	- If completion of validity of NISM certificate or Security Deposit is approaching, RA may be informed via email and/or notification.
Renewals	- RAs should be notified for renewals as per regulations. This notification should be sent out via email/SMS, and as a notification on the platform. - The application should open renewals ahead of time. - Notify RAs for renewal opening, closing dates, lapse dates, grace period dates via emails/SMS.
Annual Compliance	- Details of the Compliance officer should always be visible to the RA, with a way to connect with the officer via online methods, through the system (non-individual category only) - RAs should be able to view all compliance requirements on PFRDA platform. - Ad hoc compliance requirements: RAs should be able to view additional compliance requirements, if PFRDA asks for the same on an ad hoc basis. The system should show the documents required, and the last date for submitting proofs of compliance. - Submission of response and documents: RAs should be able to respond to the ad hoc compliance requests by writing a response and uploading the required documents. - Notifications: The system should send out notifications ahead of time, and also during the grace period. - history and logs: The system should provide a way for the user to view all previous compliance requests, their status, and logs of statuses & all documentary evidence of the same. - PFRDA team should be able to create a compliance request for an individual RAs, RAs based on certain filter criteria, or all RAs at once. Clearly defining the requirements, documents required and Date of submission of compliance.
Reports	PFRDA team shall require a reporting dashboard that displays some standard reports for RAs. - A dashboard displaying a detailed list of all RAs, with their registration status, payment status, deposit status and registration date. - A dashboard displaying the expiration date of registration for all stakeholders. - A report showing the number of renewals due and those that have been completed. - A report displaying the details of annual fee or renewal fee payments made by stakeholders. - A report displaying the information of compliance officers, including a history of changes. - NISM certificates due at various intervals

- A report displaying information on any waivers granted to stakeholders.

These reports are only indicative and shall have many similar reporting views.

PFRDA team, including business users, should be able to generate new reports by defining the metrics on their own, visualise a sample report and generate the report.

Users should be able to save a reporting format that could be made visible along with the standard reports provided by the system.

Ability to sort, filter and search data on dimensions and metrics.

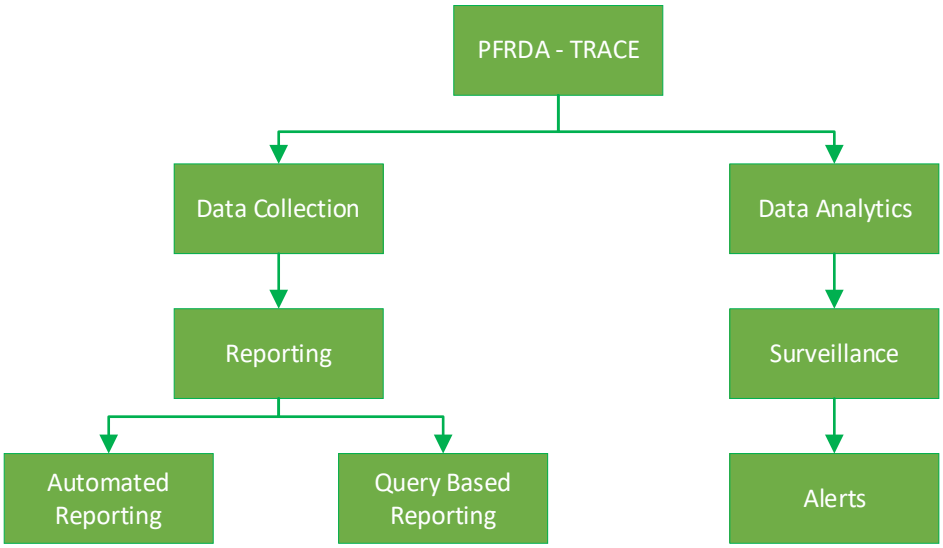
Ability to export reports in excels, CSV, via email triggers to keep a log of who downloaded the reports.

Integrate reports to other data visualisation platforms.

3. Implementing the Digital Platform for Supervisory Business Processes

Supervisory system is the system that solicits, collects, stores and analyses data submitted by various intermediaries on a regular basis. The system also provides alerts and early warnings related to imminent deadlines and any delays in the submission of data required for supervision.

Here is a functional overview of the SupTech platform that PFRDA can leverage.



4. Digitising the Supervisory Process

The system should be capable of

1. Storing Progress And Compliance Data
    a. Data which has to be referred for comparing the progress.
    b. Data which has been submitted in response to compliance and pertains to any activity carried out during the reporting period.
2. Validating the date upon submission and performs periodic reviews on
    a. MIS Returns Submitted by the Intermediaries
    b. Evaluating the exception reports (exception reports with respect to Investment Guidelines,) monthly, quarterly reports, and for internal audit reports, and proxy voting summary.
    c. Evaluating the reports on a periodic basis received from intermediaries as a part of monthly reporting.
    d. Especially on the growth in Asset Under Management (AUM), inflows, downgrades, NPAs etc.
3. Provisions w.r.t. submission of miscellaneous letters/documents may be made available to the intermediaries through the PFRDA-TRACE.
4. The partner is expected to work with PFRDA departments and standardise the report formats and simplify the reporting process. A special effort needs to be put in to ensure that redundant information from any of the intermediaries doesn't get fed in the system.
5. Each Report that is asked to the intermediary, must elaborate on why that report is being asked, at what frequency and what is the Compensation upon non submission. Each field asked for in the report should be clearly defined.
6. Ideally, the reporting interface, built on a Reporting tool, if any, must be integrated with the RegTech and SupTech interface. For avoidance of doubt, integrated means the same interface, without having to leave the PFRDA-TRACE portal. If it is not integrated, then bidder must justify the same with additional capabilities of the tool being proposed.

5. SupTech Platform

User Management	Admin role of the intermediaries should be able to define access of Users and User Roles for SupTech platform, independent of RegTech Platform.
Role Based Access Control (RBAC)	- Role assignment: Users should be assigned to roles that are defined by the system administrator. These roles are used to grant or deny access to resources. - Role-permission mapping: Permissions are assigned to each role, and users in that role inherit those permissions. - Access control: Users are only able to access resources for which they have been granted permission through their role assignment. - Separation of duties: RBAC should be able to enforce separation of duties, especially w.r.t. SupTech duties by ensuring that users with different roles are not able to perform conflicting tasks. - Flexibility: RBAC should be flexible, allowing for the creation of new roles or the modification of existing roles as the needs of the organisation change. - Auditing & Logs: RBAC should be able to provide a detailed record of who accessed which resources and when, which can be useful for auditing and compliance purposes.
Attribute based Access Control (ABAC)	- Attribute assignment: Users and resources are assigned attributes that describe their characteristics, such as role, location, department, clearance level, etc. - Policy evaluation: Access control decisions are made based on the evaluation of policies that are defined by the system administrator. These policies use logical expressions to combine attributes of the users, resources, and the context of the request to determine whether access should be granted or denied. - Dynamic access control: ABAC allows for dynamic access control decisions based on the current state of the system, such as the time of day, the location of the user, or the current threat level. - Attribute-based permissions: ABAC provides a fine-grained control over access based on the attributes of the users and resources. - Multiple policies: ABAC allows for multiple policies to be defined, each representing a different set of rules, which can be combined to make access control decisions. - Extensibility: ABAC allows for the addition of new attributes and policies without changing the underlying infrastructure.

- Auditing: ABAC can provide a detailed record of who accessed which resources and when, and the attributes and policies that were used to make the access control decision.
- Flexibility: ABAC allows for more flexibility in the way access control is handled. It enables the creation of access controls based on complex and dynamic rules, including conditions based on attributes of the user, resource, environment, and context.

6. SupTech Interface

Report Submission Interface Workspace	All intermediaries should have access to a report submission interface that will display all the reports that are pending for submission to PFRDA thus far.
Report Sections	Each Report shall have a dedicated section with the Report Title. Users should be able to view the history of reports submitted along with - Date of Submission - Submitted by (Maker) - Confirmed by (Checker) - Current Status (Submitted, Under Review, Rejected, Accepted, Needs More Info, etc) - Audit Log - Date of Review - Reviewed By - Action - Comments - Audit Logs This page shall also have any standard reporting format for reference purposes, along with dos and don'ts of submitting that report.
Data input capability	The platform should be able to accept data from a variety of sources, such as databases, spreadsheets, and manual entry, and other docs. Users should be able to upload the report in the prescribed format. The submission should accept only the prescribed format and file type. There are about 150 predefined reports that intermediaries are expected to submit at various frequencies. Users should be able to view the deadline of submitting the next report. And whether this report submission is in grace period.

Compliance Visualisation	Users should be able to see an overview of report submission and view compliance in real time. User should be able to view. - Reports that are Submitted by the Maker with validation errors. - Reports that are Submitted by the Maker without any validation errors. - Reports that are Pending for Confirmation by the Checker - Reports that are Confirmed by the Checker - Reports that are Under Review by PFRDA - Reports that are Accepted by PFRDA Successfully. - Reports that are Rejected by PFRDA and requires a resubmission. - Reports that are On Hold by PFRDA and require additional data or information. A visual representation would allow the users to drill down to the requested information and provide the same. Users should be able to click on the visual to drill down to the required section of the report section page and perform necessary actions like - Uploading new reports - Uploading an additional report or document - View comments & Audit logs - Provide comments. - Request review - And other standard functions.
Automated Data Validation	Data validation rules: The platform should be able to apply a set of predefined validation rules to the submitted data to ensure that it meets certain criteria, such as data type, range, and format. - Checks for receipt of report, its completeness, and quality. - File format: The platform should ensure that the uploaded file is in the correct format (e.g. .XLS, .xlsx) - Sheet structure: The platform should check that the excel sheet has the correct number of columns and rows, and that the headers are in the correct format. - Data types: The platform should check that the data in each cell is of the correct data type (e.g. numeric, text, date) - Data integrity: The platform should check that the data in the excel sheet is complete, accurate, and consistent. It should also check that there are no duplicate records. - Formulas and calculations: The platform should check that any formulas or calculations in the excel sheet are correct and that the results are consistent with the data.

	- Data Range: The platform should check that the values in the cells are within a specific range as per the requirement of the report. - Data Format: The platform should check that the data is in the correct format, for example, date should be in the format of 'dd-mm-yyyy' - Data Validation: The platform should check that the data matches the validation rules defined for the report. - File name: The platform should check that the file name is in the correct format and that it contains the appropriate information to identify the report. Error handling: The platform should be able to identify and flag any errors or discrepancies in the submitted data and provide feedback to the user. These increase efficiency and save time, by first cautioning the users of Intermediary organisations to confirm the data and reports they are entering are valid. And at a later stage, PFRDA team can view the validity and completeness of the report without having to spend time on it manually, only to know that the report is not ready to be reviewed. Users should have the right to submit the report for PFRDA's review, despite system cautions.
Integration with Intermediaries IT Systems	A special effort will be needed to integrate with the NPS Trust Supervisory System, to pull reports and their statuses. There are a variety of reports that are collected, validated, and reviewed by NPS Trust from various intermediaries. To avoid any duplication of efforts by the stakeholders to ask them to resubmit the report to PFRDA, these reports should be displayed into PFRDA system as and when they are submitted into the NPS Trust Platform. When the user's login to PFRDA platform, they should be able to see the reports that have been already submitted to NPS Trust.

7. Reporting Compliance Setup and Notifications Definition

Setting up a New Reporting Requirement	Admin users from PFRDA Supervisory Department should be able to set up a new reporting requirement for compliance for all, some, or a particular intermediary type. This will happen through an admin screen where the user should be able to select Intermediary Type and enter the following information. - Intermediary Type - Report Title - Purpose of the Report

	- Supporting guidelines from PFRDA Act or any other documents, justifying the need of the report. (Upload) - Report Format (Upload) - Sample Report (Upload) - Upload Frequency, in days, weeks, months, years. - Report Due Date: (one date, or recurring) - Notification template for SMS and Email for - Announcing a new report for compliance - Submission deadline - Grace Period
Notification Setup	Notifications are critical to the Supervisory System in order for the Regulator to keep broadcasting immediate needs to Intermediaries. For every report submission, PFRDA admin should be able to set up notifications independently. The user should be able to set up the following when defining notifications. - Trigger: This could be a Report Submission, Deadlines, Grace Period, etc - Notification Channel: Email, SMS, or both. - Notification to user group: Maker, Checker, PFRDA officials. - Notification Title: - Notification Text: This will also define variables. - Notification Trigger date, time - Notification Frequency: in Hours, Days, Weeks. - Notification Stop Criteria: for example, on successful submission of a report. - The system must flag the users on delays of the report and must inform the users on regular delays being made by them. The Default notifications should be pre-set into the system, and PFRDA admin should be able to edit all above variables.
Default for all reports	Email/SMS/System Alert : A feature must be available in the designed solution so that the PFRDA officials can set reminders, that could be sent at configurable time duration for submitting the report or data to various intermediaries. The notification text will contain dynamic values of Report Title, Purpose, Last Date, and other information. Once submission has been made, a notification must be sent to the submitting entity informing that the submission is done.

8. Report Submission Process

Report Submission Process for Users of Intermediaries	- Login to PFRDA SupTech System with the provided system credentials. - Data preparation: Reporting entities will need to prepare their data in accordance with the reporting requirements and guidelines provided by PFRDA. Each report will have their formats, do's and don'ts defined on the report's page. - Data submission: Reporting entities will need to upload their data to the system, either through manual entry or by importing a file in a specified format in web forms, excel, pdf uploads in defined template. - Data validation: The system will automatically validate the data using predefined validation rules to ensure that it meets certain criteria, such as data type, range, and format. This is described in one of the above sections. - Error handling: The system will flag any errors or discrepancies in the submitted data and provide feedback to the reporting entities. - Review and submission: Reporting users will need to review the data and make any necessary corrections before submitting the report. - Confirmation of submission by Checkers: After submitting the report, the system will provide a confirmation to the reporting entity, which can be used for compliance and audit purposes. - Communication around the report: PFRDA, and users communicate as the status of the report changes after each review. Both parties and post comments and respond to comments. - Report history: The system should keep a record of all the reports submitted by the reporting entity and the status of the submission.
Report Submission Statuses	- Draft: The report has been started by the reporting entity but has not been submitted yet. - Invalid: Reports that are Submitted by the Maker with validation errors - In Review with Checker: Reports that are Submitted by the Maker without any validation errors & Reports that are Pending for Confirmation by the Checker - Submitted: Reports that are Confirmed by the Checker and are submitted. - Overdue: The report was not submitted on time and is considered overdue by the supervisory authority.

	PFRDA should be able to communicate over the reports & solicit more information, if and when required. The system will have the following options built into the platform, in case PFRDA team wants to change the status flow in the future. - In Review with PFRDA: Reports that are Under Review by PFRDA - Accepted: Reports that are Accepted by PFRDA Successfully and are considered complete. - Rejected: Reports that are Rejected by PFRDA, and requires a resubmission - On hold: Reports that are On Hold by PFRDA and require additional data or information. - Incomplete: The report is incomplete, and the reporting entity has to resubmit the report after completing the missing data. - Submitted: This should be the default status once a report is submitted and waiting for any further action.
Alerts when submitting the reports	Users should be able to view the delays when uploading the reports. For example, a user should be informed that their submission is x days late. PFRDA team should be able to view the promptness or delays made by the intermediary on an average.

9. Report Submissions Frequency for Intermediaries

Report submission frequency for Intermediaries are given as below:

Table XIII.1: Report submission frequency for Intermediaries

Department	Supervision/Regulation	File type	Count) No of pdf/Sheets in excel
Points of Presence	Supervision	No. of sheets in Excel	3
	Supervision	PDF	10
RA	Supervision	No. of sheets in Excel	1
	Supervision	PDF	1
Trustee Bank	Supervision	No. of sheets in Excel	1
	Supervision	PDF	6
Annuity Service Providers	Supervision	No. of sheets in	1
	Supervision	PDF	1

Central Record Keeping Agency	Supervision	No. of sheets in Excel	9
	Supervision	PDF	8
Promotion and Development APY	NA	No. of sheets in Excel	43
	NA	PDF	NA
Promotion and Development CAB & SAB	NA	No. of sheets in Excel	6
	NA	PDF	NA
NPS Trust	Supervision	No. of sheets in Excel	22
	Supervision	PDF	18
Custodian	Supervision	No. of sheets in Excel	4
	Supervision	PDF	2
Pension Funds	Supervision	No. of sheets in Excel	6
	Supervision	PDF	3
Central Govt & State Govt	Supervision	No. of sheets in Excel	20
	Supervision	PDF	NA
Promotion and Development NPS	NA	No. of sheets in	13
	NA	PDF	NA
Market watch	NA	No. of sheets in Excel	27
Points of Presence	Regulation	No. of sheets in Excel	NA
	Regulation	PDF	2
Retirement Advisor	Regulation	No. of sheets in	NA
	Regulation	PDF	1
Trustee Bank	Regulation	No. of sheets in Excel	3
	Regulation	PDF	2
Annuity Service Providers	Regulation	No. of sheets in Excel	NA
	Regulation	PDF	1
Central Recordkeeping Agency	Regulation	No. of sheets in Excel	1
	Regulation	PDF	2
NPS Trust	Regulation	No. of sheets in Excel	NA
	Regulation	PDF	1
Custodian	Regulation	No. of sheets in Excel	1
	Regulation	PDF	2
Pension Funds	Regulation	No. of sheets in	1
	Regulation	PDF	2
		SUM	**224**

Table XIII.2: Frequency of Reports

Daily	**Weekly**	**Fortnightly**	**Monthly**	**Quarterly**	**Half Yearly**	**Annual**	**Ad Hoc**	**Quinquennial**
11	13	03	86	54	6	46	4	1

Note: The number of reports mentioned above is purely indicative. The implementation/digitalization will depend on the creation of web forms, potential variation in the data architecture and frequency of submissions.

10. Tracking & Logging Events that Disrupt Services

The software maintenance module should be designed to track and manage the maintenance activities of a software application. The module should monitor the various maintenance activities such as suspension, shutting down, merging, and other relevant activities. It will then notify the users of the application appropriately.

1. Suspension Tracking

   The software maintenance module should track the suspension of the software application. It should monitor when the application has been suspended and the reason for the suspension. It should then log the suspension event and notify the users of the application of the suspension event.
2. Shutting Down Tracking

   The module should track the shutting down of the software application. It should monitor when the application has been shut down and the reason for the shutdown. It should then log the shutdown event and notify the users of the application of the shutdown event.
3. Notification System

   The software maintenance module should have a notification system that should notify users of any maintenance activities. The notification system should be able to send notifications via email, SMS, or in-app notifications. Admin users will be able to customise the notification settings to receive notifications for specific maintenance activities.
4. Reporting

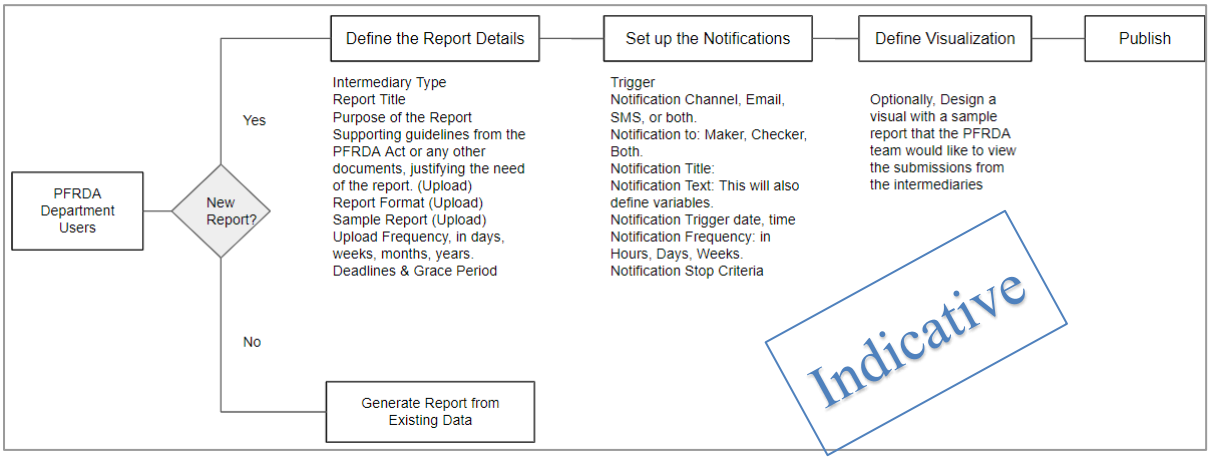
   The software maintenance module should provide reporting functionality that should allow administrators to generate reports on maintenance activities. The reports will include information such as the frequency of maintenance activities, the reasons for maintenance activities, and the impact of maintenance activities on the application.

11. Compliance Monitoring

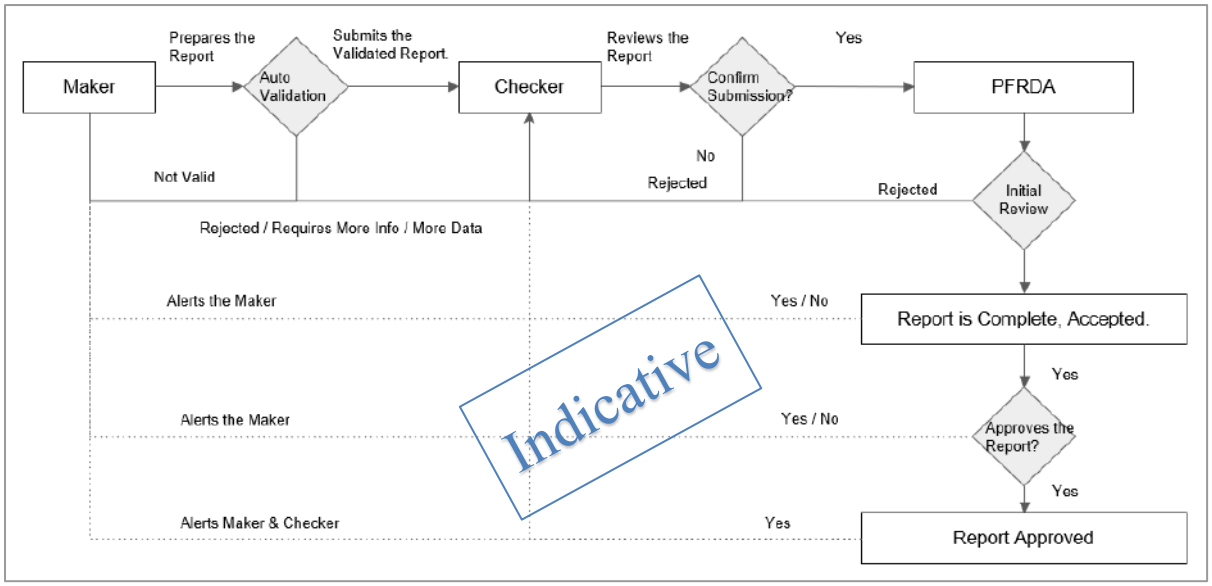
The system should allow a compliance process of capturing periodic reports issued by PFRDA from time to time, mandated by regulations/Guidelines/Circulars etc.

The solution should ensure seamless flow of data from report submission to the proposed Digital Compliance Monitoring System and generate reports/analytics reports in the format as required by PFRDA. The reports must be generated after customization as per the requirement of the functional users of PFRDA.

1. New Report Request
    a. The solution should allow PFRDA departments to request for a new compliance report, other than the ones that are routinely solicited.
    b. The user should be able to define the report. This should include a declaration about its need. The same should also have a timeline/frequency of getting generated. The report should also generate notifications for defined user groups.
    c. The sample workflow of one of the intermediaries is illustrated below for ease of understanding.

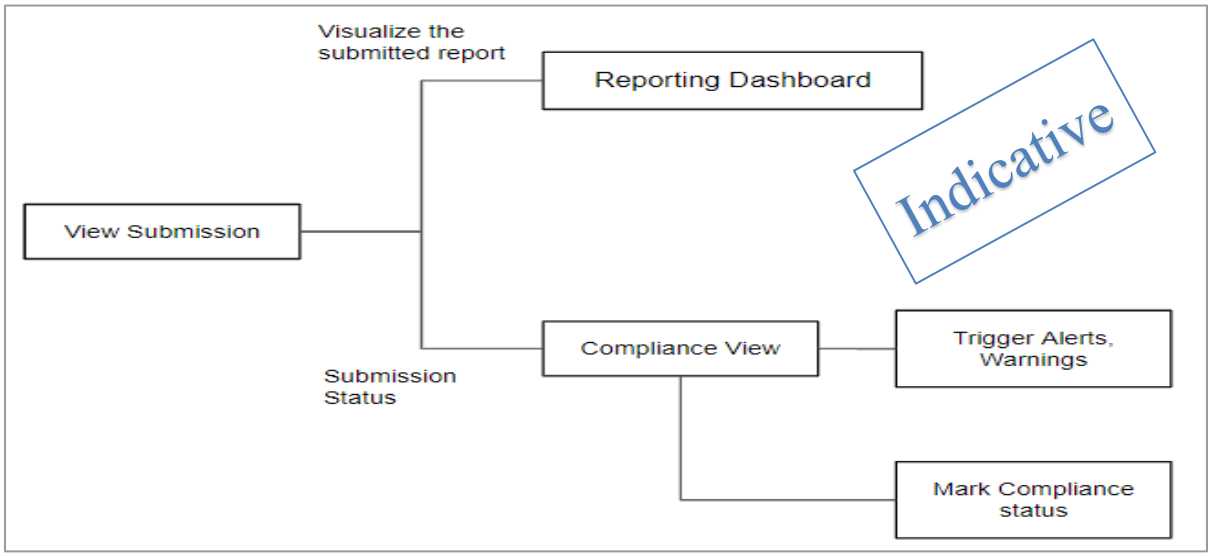


2. Report Submission
    a. The solution should provide an interface for the intermediaries in PFRDA Architecture to report in an authenticated manner with a maker/checker facility along with integration to Digital Signature Certificate technology. The interface must be user friendly to both PFRDA users and the intermediaries.
    b. System Integrator to ensure that the system is compatible to DSC standards as per Controller of Certifying Authorities (CCA) guidelines issued from time to time. Future upgradation/updation in the system to cater to revised standards as per CCA guidelines will be taken up by bidder without extra cost to PFRDA during the period of contract.
    c. The sample workflow of one of the intermediaries is illustrated below for ease of understanding.



3. View Submission
    a. System Integrator to provide a suitable interface for portal administration and report/analytics generation by associated users of PFRDA based on DSC technology as explained above.

To receive/track/follow up compliance reports to be submitted by intermediaries as per PFRDA regulations/guidelines/circulars etc., from the different intermediaries in PFRDA architecture which can be validated, consolidated, and reported to PFRDA for necessary action.



12.Publish Circulars & Advisories

The goal of this digital system is to allow regulatory authorities to publish circulars and advisories to market intermediaries, and to receive reports on who viewed or acted on them.

Circular and Advisory Management	The system will allow PFRDA Department users to create, edit, and publish circulars and advisories. They will be able to attach relevant documents, set publication dates, and defined respective intermediary.
Storage	The same circulars would be published on PFRDA website as well; therefore, the system should repurpose the documents storage being used for the website.

13.Key Objectives of the Data Warehouse, BI & MIS layer

PFRDA receives data from various intermediaries using emails or physical files and a variety of different formats at different times. It is a very tedious task to identify errors and consolidate data manually using spreadsheets for various intermediaries. Data storage on a central platform will minimise these pain points and generate significant benefits for various departments. The target architecture should include a data warehouse to store, curate, and aggregate data from various intermediaries, external entities, and internal applications and ensure that it is available for standard reports, ad hoc reports, analytics. Any data related to this system shall be exclusive property of PFRDA.

The following are the key high-level service objectives PFRDA expects to achieve through Data and Analytics Platform:

1. **Dashboard** : The Data Warehouse and Analytics Platform, plays a pivotal role in enhancing the Pension Fund Regulatory and Development Authority's (PFRDA) data-driven capabilities. Within this platform, the Dashboard component stands as a crucial segment, providing a comprehensive panoramic view of intermediary activities, cross-intermediary interactions, and department-specific functionalities, covering research, supervisory, regulatory, promotion & development, as well as training & development initiatives. This Dashboard serves as a dynamic and centralized hub, facilitating insights and data visualization, enabling PFRDA to make informed decisions, monitor activities, and drive strategic initiatives with precision and efficiency across all facets of its operations.
2. **Data Warehousing**: The platform to include a robust data warehousing solution for compliance data. This should facilitate ad-hoc queries and report generation.
3. **Report Automation:** It should automate the generation of standard reports, reports needed for regulatory policy formulation and promotion and development activities.
4. **Data Analytics Tools**: The system should be equipped with analysis capabilities and data visualization tools to uncover insights from the report data.

5. **Customized Reports**: The platform to allow for the creation of customized reports at user end using dashboarding tools, catering to the specific needs of different departments.

The Data Strategy encompasses the following elements:

1. **Data Extraction**: System should be capable of extracting data and reports from the specified data sources. Mechanism & formats will be specified for intermediaries for data transfer to PFRDA.
2. **Data Export and Sharing:** System should be capable of data export & sharing as per the details as mentioned as below**:**
3. **Data Export**: The system should allow users to export reports and data in various formats, including PDF, Excel, and CSV.
4. **Data Sharing**: Users should be able to share reports and dashboards with authorized stakeholders.
5. **Embedding**: The BI-LAYER should support the embedding of reports and dashboards in external applications or websites.
6. **Data Retention:** The proposed solution should be capable of long-term data retention. PFRDA should be able to store historical data and maintain data for compliance, auditing, or future analysis without significant costs.

14.Data Visualization & Analysis Capabilities

Data visualisation	The system would need to provide various types of interactive visualisations such as line charts, bar charts, scatter plots, heat maps, and dashboards, to help users understand and analyse the financial data. - The users should be able to apply filters of date range, segments & demographics wherever applicable. - The users should be able to sort the data on all dimensions of the reports. - Drag & drop interface for data transformation & preparation. - Comparative Analysis capabilities over two date ranges to ascertain week-on-week, month-on-month, and other similar comparison of a dimension/report. - Automated data refreshes - Drill Down capabilities (ability to drill down to various levels of a hierarchy) - Able to format (page size, row, columns, fonts, colours, tables etc.), allow data processing (slice & dice multidimensional data on the fly, pivoting, sorting, ranking etc.) - User friendly GUI to allow easy generation of reports and exporting. - A device agnostic web interface to view reports. - Built-in ETL and/or strong integration with leading data preparation platforms.

	- Compatible with all environments like Windows, Linux etc. - Capability to embed visualisation. - Provide native access to leading RDBMS solutions and capability to connect with big data components. - Facility to save the queries and edit the same in future to derive newer queries. - Supports object level as well as row level security. - Cross-platform and Cross-device access Mobile Integration/Support for iOS, Android.
Customizable reporting	- The system should allow users to create custom reports by defining the metric on x-axis, y-axis and defining the measures. This could be done by showing to the user's available tables, keys and foreign keys & users choosing the metrics from each table they want to combine. - The system should allow choosing from a variety of visualisations such as bar chart, line graph, pie chart and other standard visualisations provided by popular visualisation tools. - The user should be able to save the customised report, and make it visible to oneself, or have the organisation view it.
Data querying and exploration	- The system would need to provide users with an easy-to-use interface for exploring and querying the data, such as a search function or advanced filters. - Advanced Technology Users should be able write queries and datasets to retrieve data and turn it into visual reports.
Sharing & Collaboration	- The system should allow users to share their insights and visualisations with other stakeholders, and to collaborate on them in real-time. - The users should be able to leave comments on the reporting view and tag peer users to trigger email notifications to them. - The users should be able to view all comments and filter comments by username, sort by latest or oldest.
Alerts & Notifications	- The system should allow users to set up alerts and notifications based on specific conditions or events in the reports. - The users should be able to create email notification for any report by entering their email ID, frequency, and trigger condition. - The system should have capabilities to alert concerned users of PFRDA for any frequent change of the users by intermediaries.
Data Export	- Every time the users try to export a report, the following workflow must be triggered. - The user expecting to download the data should be shown her/his email ID displayed on the user interface, either confirm or edit the same. This can be picked from the user's logged in account.

- After confirmation of the email, the user should be able to select the report format, for example, csv, XLS, pdf, doc, and other standard formats. While selecting the format, the default format should be suggested to the user.
- Upon confirmation of email and format, DO NOT download the report from the browser session, instead mail the same report as a password protected attachment, and send another email with the password following the email with attachment. The super admin, or a defined email ID, should be kept in CC/BCC to keep a track of when & who is downloading the reports.
- PFRDA team, should be able to view a log of report exports in a tabular view with the latest on top, mentioning the user, email, file type, send time, open time, forwarded time, forwarded to, etc and other standard parameters to keep a track of movement of the reports and to ensure security.

Schedule III – Indicative Technical Specifications

1. Architecture Boundaries

The e-PLATFORM should offer a centralized repository, collaboration tools, reporting & BI, Analytics, Business rule engine, robust security, integration capabilities, reporting, an intuitive interface, compliance with industry standards, scalability, and cost-effectiveness.

a) Technology Architecture

This RFP section is dedicated to delineating the desired PFRDA system solution architecture, allowing for flexibility and adaptability to accommodate future improvements based on ongoing learning and requirements evolution. It aims to define the expected technical architecture, firmly rooted in internationally accepted standards like The Open Group Architecture Framework (TOGAF), while also promoting the system integrator (SI) innovative contributions and suggestions to enrich and optimize the proposed architecture.

b) High-level design principles

The design for the solution architecture for PFRDA needs to follow the following broad architecture Principles, but not limited to:

1. Loosely Coupled Architecture
2. Scalable and Flexible
3. Repeatable and Reusable Components
4. Automate as much as possible.
5. Aligned with Business Strategies, Processes & Technologies
6. Cost-effective
7. Self service as core focus

c) Guiding Architectural Principles

IT architecture principles defined in this section are the underlying general rules and guidelines that will drive the subsequent development, use and maintenance of architectural standards, frameworks, and future state target architecture. SI may include the following components for architecting an efficient, scalable, robust, cost-effective solution for this RFP.

Architectural Principle	Explanation
Cloud Neutral	Ensure the solution is cloud neutral and no cloud native services are being used that are not migratable.
Containerization	Employ containerization to package applications and their dependencies. This ensures consistent deployment across various environments, enhances scalability, and streamlines management.
Cloud-First Approach	Prioritize cloud computing as the foundational infrastructure, enabling flexibility, scalability, and cost-efficiency. Cloud services facilitate rapid development, testing, and production deployment, reducing capital expenditure.
Commercial Off-The-Shelf (COTS)	Embrace COTS solutions to expedite project delivery. These pre-built software products require minimal customization, reducing development time and costs.
Modified Off-The-Shelf (MOTS)	When necessary, consider MOTS solutions, which allow for the customization of COTS software to meet specific project requirements. This balance combines the benefits of pre-built functionality with tailored features.
Infrastructure as a Service (IaaS)	Leverage IaaS to access virtualized computing resources, including servers, storage, and networking. This approach provides a flexible foundation for application hosting while the cloud provider handles services maintenance.
Platform as a Service (PaaS)	Implement PaaS to simplify application development and deployment. PaaS solutions offer pre-configured development environments, frameworks, and tools, allowing developers to focus on coding rather than infrastructure management.
Software as a Service (SaaS)	Utilize SaaS solutions for delivering software over the internet. SaaS applications eliminate the need for local installation and maintenance, offering rapid deployment, scalability, and reduced IT overhead.
API Studio	Establish an API Studio to systematically design, develop, and manage APIs. This tooling and practice enhance interoperability, security, and reusability, facilitating efficient communication and integration between systems and services.

Architectural Principle	Explanation
Microservices Architecture	Adopt a microservices approach to decompose applications into smaller, independently deployable services. This architecture enhances scalability, resilience, and the ability to update components without affecting the entire system.
Serverless Computing	Explore serverless computing to execute code in response to events without managing server infrastructure. This approach minimizes operational overhead and allows for rapid development of event-driven applications.
Data Security and Compliance	Prioritize data security and compliance with relevant regulations, ensuring data protection, encryption, and access control measures are in place, especially for sensitive information.
Continuous Integration/Continuous Deployment (CI/CD)	Implement CI/CD pipelines to automate software delivery and deployment. This approach improves code quality, accelerates release cycles, and reduces manual intervention in the software delivery process.
Scalability and Elasticity	Architect systems to be highly scalable and elastic to adapt to changing workloads and usage patterns, ensuring optimal performance and resource utilization.
Monitoring and Analytics	Incorporate comprehensive monitoring and analytics tools to provide real-time insights into system performance, user behavior, and security, enabling proactive issue resolution and data-driven decision-making.
DevOps Culture	Foster a DevOps culture emphasizing collaboration between development and operations teams, promoting automation, continuous improvement, and a shared responsibility for the software development lifecycle.
Open Standards and Interoperability	Embrace open standards and promote interoperability to ensure that systems and components can work seamlessly together and facilitate integration with external services.
Data Privacy and Consent Management	Implement robust data privacy and consent management mechanisms to comply with Indian data protection acts, regulations & guidelines for user privacy rights, including data access and deletion requests. In addition

Architectural Principle	Explanation
	to aforementioned compliance, SI may refer Global best practices in Data Privacy domain.
Data Access Management Tool	A Data Access Management (DAM) tool is a software solution or system designed to regulate and control access to data within an organization. These tools focus on managing user authentication, authorization, and auditing to ensure that data is accessed and utilized only by authorized individuals or systems.
File sanitization	File sanitization is the process of removing sensitive or harmful information from a file to ensure data security and privacy. This involves techniques such as metadata removal, redaction, and encryption to prevent unintentional disclosure of sensitive content. The goal is to minimize the risk of unauthorized access and comply with security and privacy regulations.
Disaster Recovery and Business Continuity	Develop and implement disaster recovery and business continuity plans to ensure system resilience in the face of unexpected outages or catastrophic events.

Table 1: Architectural principles

PFRDA system would be built on the following core principles:

#	Principle	Description
1	Open IT/ Ecosystems	- Well defined APIs are designed with open standards. - Easily integrate new systems, - Standards-based and open. - Enable new ecosystems to extend the breadth and depth of offerings
2	Minimise Architecture Complexity	- Use applications/tools for core purposes, not for what it can do. - Pre-integrated components are designed to work together. - New vendors/services are only introduced if the capability is not available from the existing platform or is differentiating.
3	Rapid Delivery	- Supports modern engineering practices (DevOps, Agile, Containerization). - Frequent, incremental, and instantaneous updates are in line with the platform roadmap. - Consume non-differentiating “Utility” services via API.

#	Principle	Description
4	Configurable & Extensible	- Business self-service for 'business as usual' changes (configuration changes). The Self-Service theme is critical at all times. - Extensions do not compromise the upgrade path.
5	Scalable	- Can be supported in any appropriate clouds. - Available in an 'As a Service' model – available and scalable. - Scales up and down easily for consumption peaks and troughs.
6	Information-Centric	- Uses data and insights to drive behaviour. - Easily shares information and insights across the architecture. - Systems must publish their data with technical and business metadata. - Reduce latency of data ingestion and consumption and maximise reuse potential (the right data at the right time). - Configuration-driven and self-service data integration services. - Data consumption services to enable reuse of integrated data, reduce uncontrolled growth of 'stovepipe solutions' and enable flexibility for self-service consumption.
8	Manageable & Supportable	- The platform supports continuous availability and can be updated without downtime. - Supports phased implementation of new features.
9	Compliant, Secure and Reliable	- Data collected, stored, or processed meets the data protection policies and is managed and backed up in accordance with data management policies. - Designed with the principle of least privilege – provide role-based access to information and resources for users or services where a legitimate purpose is identified. - Ability to support discrete asset/function security models, e.g., Microservice security.
10	Cloud	- No cloud lock-in. - Support application delivery controller technologies; global load-balancer, traffic proxy, etc. for cloud workload control. - Ability to use service discovery mechanisms for transparent, loosely coupled service integration.

Table 2: Core principles

d) Solution Architecture

PFRDA platform should be a highly flexible microservice architecture in order to satisfy business requirements in minimum time for development and minimum disruption. The target state architecture should cover three aspects: architecture, software design and DevOps.

The architecture with an API layer to decouple services by Introducing DevOps and automate everything into a highly flexible cloud container solution to get the services developed as quickly as possible.

Each aspect should cover specific tasks in order to enable microservices across PFRDA functional modules.

Architecture:

Identify the functional domains of the application landscape.

1. Define business driven API landscape along the identified functional domains.
2. Encapsulate the monolith with thin microservice layer to provide the defined business driven APIs.
3. Define robust guidelines for the integration of the microservices (i.e., RESTful)
4. Introduce an API management platform to provide a common set of functionalities.
5. Define the allowed database and storage patterns.
6. Define data archival design as per the data archival policy.

Software design:

Detail each function into different contexts in the application.

1. Separate the contexts into logical blocks.
2. Build the logical blocks as modules.
3. Carve out modules from the application as microservices.
4. Do this incrementally.
5. While writing the code, standard practice to be followed like –code commenting.
6. Separate the frontend from the backend layer if those are currently combined in a full stack application.

DevOps and automation:

Introduce DevOps methodologies:

1. Automate integration, testing and deployment with CI-CD pipeline.
2. Automate infrastructure provisioning with cloud technologies.
3. Use containerization to maintain separation between the microservices.
4. Set up central logging and monitoring to get rapid feedback about usage, errors, and cascading failures (can be provided by API gateway).

PFRDA platform should go for defining a layered architecture with defined components.

1. The target architecture is expected to have well defined layers of responsibility. Each layer is expected to implement a specific purpose and should not overstep its responsibilities such that it encroaches the responsibilities of the other layer.
2. The layers are expected to communicate with each other using well defined protocols and data structures. No hard dependencies between the layers should be there.
3. In the following sections, we have provided an overview of the responsibilities/architectural considerations for the various components contained in the layers in question.

e) Domain Layer

The Domain layer should be built using 6 architectural constructs. The same are described below:

1. Microservice architecture :
    a. The architecture should be developed in order to have essential architectural elements – "Code & data isolation with centralised configuration" , " Service discovery, registry and centralised monitoring" , " Horizontal scalability, automated deployment".
    b. The target architecture needs to be domain driven, and merely based on the specific needs of each screen of the UI.
    c. Separate code and data-isolation (database schema) for each domain services adhering guidelines of domain driven design.
    d. Each microservice should have well defined domain boundaries. Services need to be highly cohesive and should not step over the functional boundaries of another service.
    e. There should not be any hard dependencies or hard relationships between entities belonging to separate micro services. Only soft dependencies will be maintained between entities of different micro service.
    f. Each domain service should perform its transaction and publish an event. The consumer should listen to the event and perform transactions. If the transaction fails for some reason, a failure event should be thrown to roll back the transaction in another service.
    g. During varying traffic needs for read and write operation, target architecture should support Command Query Responsibility Segregation (CQRS) principle.
    h. For high availability, each microservice should be able to scale horizontally.
    i. Each microservice should have a separate code base in the version control system.
    j. Each microservice should have a separate schema with access to its own schema.
    k. All microservice should be configured under CI-CD pipeline for build steps and when deployed, it should fetch configuration from a central config server.

l. All microservices should register their availability status, base-URL to a central service registry allowing other microservice to communicate.

m. The architecture should be defined for an event driven system.

n. The architecture should be horizontally scalable – using the principles of CQRS, events and composable workflows.

o. In order to share master data and configuration, distributed cache should be implemented. Container orchestration tool to support cluster deployment with failover mechanism to switch from node to node in case of failures.

p. Microservice deployment should happen through CI-CD(continuous integration, continuous deployment)

q. Architecture should have monitoring and fault tolerance using a log tracing mechanism with unique trace IDs to keep track of requests being routed to multiple services.

r. Target architecture should implement capabilities to aggregate logs from different microservice to a central log viewer for easy access and analysis. This implementation should allow searching, filtering logs based on service id, log levels, origin, timestamp etc.

s. The microservice architecture implementation should have well defined strategies for fault tolerance. This fault tolerance architecture should ensure fault tolerance by ensuring a strict timeout policy per request from waiting forever, a circuit breaker policy preventing repeated failure by setting some condition to activate circuit breaker.

t. The architecture would work with events generated from various state/process changes, in turn would inform the related services.

u. Each service should subscribe to events with event data in well-defined data structures.

v. Interaction between the services would happen via events, composable workflows. The architecture would not facilitate any point-to-point interaction between the services.

w. In order to save all the changes to the data state, the event store has to be defined, in order to capture the state change in the form of event streams.

x. In order to orchestrate complex business processes, composable workflows using workflow/ Business Process Modelling and Notation (BPMN) engine to be built. This would avoid hardcoding of workflows in the microservices.

y. Workflows would be exposed using API based interfaces and would be independently deployable and testable.

z. Standardise definition of data dictionary to form a uniform repository of master data elements to be referenced with all PFRDA service & 3rd party systems.

aa. The master data dictionary would establish a common vocabulary for internal and external communication. The data elements would include product codes, data codes for product specs, geo-codes, etc.

bb. Master Data Management/MDM systems should implement a hierarchy between related data which employs parent and child relationships. An example would be state and district.

cc. Master should have standardised format and should be readily available to all components.

dd. Master data should be present in distributed cache for faster retrieval.

ee. Master data management should support multilingual capability.

f) Integration Layer

1. Integration with External System

PFRDA platform integration process should work for inbound and outbound data exchange mechanisms with external systems.

1. For the outbound integration process, usage of process automation with well-defined contracts (via channel adaptor) and usage of proxy pattern by defining a contract layer. The contract layer should be kept different from the domain service layer to ensure loose coupling between invocation from domain service to 3rd party system and its implementation.
2. For inbound integration process, a well-defined interoperability framework needs to be built in the architecture framework:
    a. Definition of data interchange standards,
    b. Master Data Codes, and
    c. Requested signatures that can be used to integrate with PFRDA platform.

The platform should ensure definition of standard interfaces, data-formats, and protocols. In order to exchange data and services securely – modular web services to be exposed by PFRDA platform & API gateway to as single point of entry and exchange for any 3rd party data exchange.

Integration Technologies that are recommended to be used are:

1. JSON/XML based data exchange on RESTful Microservices API/Thrift API
2. Standardised API structure/framework as exposed by PFRDA to be consumed by external systems.
3. Proprietary contract layer (channel adapters) for e.g., JMS, web-services, SFTP, etc.

Connection with external applications should be provisioned via a common messaging system using messages of a predefined format. The messaging style should maximise decoupling between systems not only from the interface perspective but also from a time-based perspective. Some of the common patterns to be followed – Pub/Sub, Event message, channel adaptor.

2. Replication technologies for replication of data between different data stores:

1. Interfacing mode for PFRDA platform will be leveraged as real-time in most of the cases, while file transfer & point to point in some cases. The messaging could be synchronous/asynchronous with external or third-party systems. The following integration target points could be considered for interface design :
    a. SMS & Email application, acting as the SMS & Email Gateway, will make use of APIs for SMS & email communication, which can be both event-driven as well as time-driven. The API will be exposed to initiate the broadcasting or alert notification.
    b. Message based interfacing technique will be leveraged for real-time asynchronous integration mode. The following integration points could be considered for message-based interfacing.
    c. Data integration in batch mode will be through ETL using dimensional modelling and data pipelines. The following integration points could be considered for ETL data integration –
2. Initial data migration to cleanse, validate and load the data into target tables.

   Only Incremental data load from all the individual transactional systems to central enterprise data warehouse solutions for aggregation, mining, dashboard reporting and analytics on a periodic basis for e.g., daily/weekly/monthly refresh cycle.

g) API Gateway Services

It is expected that the communication of PFRDA services – domain, application and workflow engines with external interface will happen through an API layer. An API gateway to be used as a single point of entry to manage the API communication with the external interfaces. Following are some of the expected features for API management using API gateway -

1. All access to PFRDA platform backend system will be via microservices. Access to microservice will be via an API gateway.
2. API gateway can be implemented using available tools.
3. API gateway should implement cross cutting concerns like logging of request, idempotency, request throttling, security for request authentication, monitoring/metrics across microservices.
4. The API gateway implementation should be based on a reactive programming model with circuit breaker integration, load balancing, service discovery.
5. API gateway implementation should have an ability to match routes on any specific routes, pre and post filters which can be either global or specific to any routes.
6. All the APIs would be stateless in nature, thus easy to load balance, even if the hit through portal is extremely high and this requires high end processing.
7. All the APIs, both internal and external, should be on HTTPS or secure protocol.
8. The API gateway should be allowed to manage all enterprise initiatives from a single solution.

9. The API gateway should support existing APIs and developer preferences and provide the features in line developer preferences.
10. The API gateway should provide clustering and ensure reliability, scalability, and single point of administration.
11. The API gateway should provide for enterprise grade encryption.
12. The API gateway should provide secure access to all APIs and provide all the forms of authentication, access control and certificate/credential support.
13. The API platform should provide comprehensive threat protection for all API traffic.

h) Security Architecture

This section recommends the proposed security architecture aligning with the overarching architectural principles. The basic tenets of PFRDA security architecture are the design controls that protect confidentiality, integrity and availability of information and services for all the involved stakeholders. The security controls are defined for 6 layers, namely, Business, Data, Application, Perimeter, Network and Endpoint.

For designing PFRDA's Security Architecture, following principles need to be adhered to:

1. Data Integrity: PFRDA data must be correct, consistent, and un-tampered.
2. Data Privacy and Confidentiality: Information needs to be shared on a Need-To-Know basis and shall be collected/accessed/modified only by authorised personnel.
3. Non-reputability: PFRDA should ensure non-reputability of information in the system.
4. Secure by Design: Security has to be built into all stages and all aspects of architecture development, based on Zero-trust principle.
5. SI shall be responsible for meeting project's comprehensive security requirements and 24*7*365 monitoring, analysis, and management to ensure adequate security posture & security compliances as part of its security operations activities (through a SOC). However, PFRDA reserves the right to further appoint an external agency for monitoring the compliance to security requirements by SI. The external agency shall have access to security tools deployed by SI (at no cost to PFRDA) as part of the RFP.
6. In the proposed solution architecture, SI to ensure that data storing & processing happens according to **THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 (NO. 22 OF 2023) for meeting various business output goals of PFRDA.
7. In the proposed solution architecture, SI to ensure that they incorporate Extended Validation (EV) SSL certificates for the web infrastructure. The EV SSL should ensure the highest level of user trust and security, validating not only domain ownership but also our organization's legitimacy. Bidders should detail their experience with EV SSL deployment and provide a comprehensive implementation plan.
8. Endpoint Detection and Response (EDR): SI should ensure that an integrated, layered approach to endpoint protection that combines real-time continuous monitoring and endpoint data analytics with rule-based automated response should be a part of the security framework for the designed solution.

1. Business Layer

Based on the business requirements SI should develop policies and procedures to have secured solutions. Risk assessment, stakeholder identification, asset identification, the requirement of every service and application, various standards and statutes are required while designing security policies. At the business layer SI should do risk assessment followed by the impact analysis of these risks to identify appropriate controls and define them in the security policy document.

i. Defining Policy

1. Responsibilities of PFRDA
    a. Brainstorm, provide relevant inputs, and review the policy proposed by SI.
2. Responsibilities of SI
    b. Develop the security policy to address threats and vulnerabilities. SI would need to advise and comply with the policy.
    c. Identify the resources to implement, monitor and update the security controls as per the defined policy.
    d. Define the schedule of regular testing and monitoring to maintain to ensure all-time security.
    e. Define the access controls at various levels such as data centre, application, data, network, peripheral layers.
    f. Define authentication mechanisms at various levels as per the business requirements.
    g. Define compliances related to endpoint usage.
    h. Define cryptographic standards to be followed along with the recommended key management policy.
    i. The security policy document should be published and made available for ready reference for all the concerned.

ii. Functionality at Business Layer

1. Security architecture and design: A proper security architecture considering all the components as per the reference model should be in place and configurable design to meet the objectives of the overall security of the enterprise.
2. IT security governance: This comprises formulation of guidance, structures, and processes for implementation of IT policy, risk, compliance, and audit functions.
3. Threat Modelling: What are the threats and what can be their sources should be identified? In order to do threat modelling identification of assets and related vulnerabilities is crucial.
4. Risk assessment and management

a. Assets should be first identified and then the Inventory of assets should be maintained. Acceptable use of assets should be documented and ensured that it is implemented.
b. Information should be classified as per its sensitivity and risk associated with the information such as data leak, privacy etc.

5. Security technology evaluation: The objective of security technology evaluation is to determine the degree of compliance with a stated security reference model, various controls, standards, and specifications. For example, Common Criteria for Information Technology Security Evaluation (abbreviated as Common Criteria or CC) is an international standard (ISO/IEC 15408) for computer security; Information Technology Security Evaluation Criteria for evaluating enterprise security are being used extensively.
6. Continuous monitoring and analysis: It is not only defining the policies, standards or referring of the various international security standards but also defining the metrics which should be monitored and analysed on a regular basis to achieve the required quality for security.
7. Security training to build awareness: There is a need to develop a proper plan, policy to create awareness, capacity building for achieving the desired security for an enterprise.
8. Incident detection and handling: The purpose of incident detection and handling is to determine the possible attacks/threats to the overall system. Vulnerability at any level of the reference model can lead to a threat to the overall system. There should be a mechanism to identify that vulnerability and the procedures to handle them. For example, vulnerabilities related to network security, physical access to the systems, data access management etc.
9. Continuous certification and accreditation of policies
    a. SI should conduct the audit at regular intervals to verify the conformities. External agencies will be appointed for auditing and SI should fully support to ensure that the audit is completed smoothly and on-time.
    b. The report of the audit must be reviewed by the SI & PFRDA for action and up-gradation required.
    c. Non-conformities identified during the audit should be addressed by SI and used for corrective action as well as improvement in the policy.
10. Escalation management of security incidents
    a. All information security roles and responsibilities should be identified and allocated to the appropriate people.
    b. Appropriate contacts with the relevant authorities should be maintained.
    c. Maintaining a security dashboard.

iii. Business Layer Controls

Some basic controls related to the business layer are mentioned in this section. This is to be noted that the list of controls defined in this document is not a complete list but a guideline only. More controls should be defined as necessary. The below table provides the list of essential controls at the business layer of the security model.

Business layer controls	**Description**
Access Control Policy	- A policy should be established, documented, and reviewed as per the business information security policy to provide access to information or assets available at the organisation/department level. - The policy should define who can access what resources and what authentication mechanism should be used to provide the access. - Different multi-factor authentication mechanisms should be defined for accessing different information and information facilitating resources based on sensitivity. - The principle of 'Least Privilege' shall be followed, so as to give only the minimal permissions and authorizations to any user to enable him/her to perform the specified functions.
Strong password	- The policy should define what is an acceptable password. A strong password is recommended with a minimum of 8 characters, with at least one capital character, at least one numeric and at least one non-alphanumeric character.
Professional/company email id	- It should be mandated that for all the official work only the company/department email ID should be used.
Incident reporting and handling	- A mechanism should be defined and made available to detect any security-related incident. - A procedure should be well defined and documented giving steps to be taken for handling any incident.
SIEM	- SIEM has two components, SIM (Security Information Management) and SEM (Security Event Management). It should provide real-time analysis of the security alerts generated by network services and applications.

Business layer controls	Description
	- A software information and event management system should be defined and documented for handling security-related incidents.
Learning from the security incidents	- Knowledge gained through analysis of the earlier incidents should reflect in the security policy document.
Continuous Monitoring	- An institutional setup consisting of information security experts should be established for continuous monitoring that can help in detecting any security-related incident. - The monitoring also includes the analysis of all actions and detection of the integrity getting compromised anywhere in the enterprise.
Policy for cryptographic control usage and key management	- The security policy should include the use of cryptographic controls to ensure the confidentiality and authenticity of the user as well as systems. - The security policy should document the secured use and storage of cryptographic keys. - The cryptographic keys should be changed at regular intervals. The security policy should define the interval at which the keys are changed. The policy also should document the key generation mechanism to be used
Installation of software	- A secure procedure should be defined for installing software. - Rules governing the installation of software should be defined and implemented. - Vulnerability Assessment and Penetration Testing (VAPT) should be mandated before installing any software in the production environment. Many CERT-IN empanelled agencies do VAPT testing of applications. - Separate development, testing, staging and production environments should be recommended.

Table 3: Business layer controls

2. SIEM

Even after the risk analysis, identification of threats and providing controls, security breaches may happen. These are referred to as security incidents. There should be a well-defined mechanism to detect such incidences and reporting of these. Such incidents are analysed by professional bodies such as CERT-IN. The professional body after analysis of the incident may publish an advisory. The security policy should be modified as per the recommendations given in the advisory. Updated security documents should result in appropriate controls at various layers to prevent the recurrence of the incident.

3. Perimeter Layer

Access to any software is restricted first through the services where it is deployed. The environment in which the data and the application reside should be protected first. Physical security is vital in order to protect the information and resources from unwanted access and intrusion.

4. Functionality at Perimeter Layer

The main functionalities at the Perimeter layer are to identify the appropriate security for every asset, application/service, and data. Based on the policies defined at the business layer regarding the access to various assets, the appropriate configurations at various levels should be done at this layer.

1. Secure DMZ – Design the network considering the sensitivity zones.
2. IDS/IDP – Intrusion detection and prevention at the physical layer
3. Firewalls – to protect the infrastructure from unwanted or blacklisted intruders.
4. Message Security (anti-virus, anti-malware) – Appropriate antivirus and anti-malware should be identified and deployed. Policy regarding the same should be made to inform all the concerned. A hybrid OS may be implemented to avoid ransomware.
5. Data Loss Prevention
6. Buffer Overflow Exploit Protection

5. Controls at Perimeter Layer

The table below gives some of the important controls that should be considered while designing the security at the data centre.

Objective: Secure areas- To ensure that the information and the assets are not accessed, altered by unauthorised users through securing access to the physical infrastructure and the environment.		
1.	Security of network services	Security mechanisms, service levels, and management requirements of all the network services should be identified and included in the service level agreements.
2.	Avoid single point of failure	In-network paths between users and critical IT system resources, all the links, devices (networking and security) as well as servers should be deployed in redundant configurations (also known as High Availability – HA).

Table 4: Perimeter layer controls

6. Cyber Intrusions and Security Controls

The rate of cyber-crimes has increased drastically as the usage of online applications through various channels has increased. Different techniques are applied to prevent cyber-crimes which include the access control mechanism, providing only authorised access, putting restrictions on the use of assets, applying different techniques to secure the data in storing or in transition, intrusion prevention systems etc. Still there remains the possibility of intrusion and it should be detected and then managed. For detecting such intrusions intrusion detection mechanisms are used at the information level. Once the incident occurs, it should be managed and the changes in the security controls should be done accordingly. Controls related to incident management are given below. Cyber security controls are required at the perimeter, network as well as end-point layer.

Management of information security incidents and improvements

Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.		
1.	Responsibilities and Procedures	SI responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to information security incidents.
2.	Reporting information security events	Information security events shall be reported through appropriate management channels as quickly as possible.
3.	Reporting information security weaknesses	User of the organisation's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.
4.	Assessment of and decision on information security events	Information security events shall be assessed, and it shall be decided if they are to be classified as information security incidents.

5.	Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.
6.	Learning from information security Incidents	Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.
7.	Collection of evidence	SI shall define and apply procedures for the identification, collection, acquisition, and preservation of information, which can serve as evidence.

Table 5: Management of information security incidents and improvements

7. Audit

An internal audit should be conducted by SI at regular intervals to monitor the security of the system and applications/services. SI should have well-defined requirements and should conform to a certain standard, and to ensure the conformance to various defined security policies and as a preventive measure of prevalent security threats, a security audit would be performed.

1. The goal should be defined for the audit. For every audit criterion and scope should be well defined.
2. SI should define a plan, frequency, method, and reporting structure for the audit. While designing the audit program, the importance of the process should be taken into consideration, results or reports of the previous audits should be considered.
3. Various audit reports should be preserved for reference.
4. PFRDA has the right to appoint an auditor, internal or external.

Audit Considerations		
Objective: To minimise the impact of audit activities on the production environment.		
1.	Audit Controls	Audit activities involving verification of systems in the production environment should be carefully planned to have minimal disturbance to the business or service.

Table 6: Control related to audit.

While performing the security audit of services or infrastructure, the testing is performed on the production environment. Hence, it should be designed carefully so that it will not affect the services.

8. Recovery Strategy

Disaster recovery is an important aspect of information security. In the case of any natural or man-made threat, the earlier data should be made available.

Availability		
Objective: To ensure the availability		
1.	Availability of Information facilitating infrastructure	Information facilitating infrastructure redundancy sufficient to make the availability requirement of the application should be ensured.

Table 7: Recovery controls

Business requirements for the availability of the service/application/information system should be identified. In order to ensure 24 X 7 availability, a redundant infrastructure should be identified. This infrastructure should also be tested for a failover mechanism.

9. Network Layer

The perimeter layer covered the storage aspect of the application, service, or data. However, the data in transit needs to be secured through the network layer. Many functionalities at the perimeter and the network layer are common.

10. Designing of Network

Network Security is critical for IT systems and their proper operations as most applications work in the networking environment and closely depend on network performance, reliability, and security. Improper network design can be expensive i.e., loss of business, data loss, security breach, costs of network restoration, etc. Essential to network design is the security architecture that describes the network segmentation (i.e., security zones) and security layers (i.e., access control, intrusion prevention, content inspection, etc.).

11. Logical Network Segmentation

The network should be designed as a "Zero Trust network" based on the trust level requirements of the application or the department or the service. While designing a network, the first one should identify different trust level applications or systems. Indicative design factors :

1. Untrusted zone (Internet/Outside Access) - It is the zone through which the organisation/department/state connects to the outer world of the internet through Internet Service Provider (ISP).
2. Low Trust (External) - The systems deployed in this zone should be tightly controlled and hardened to reduce the attack surface. External DMZ has systems that are exposed to the internet for public access such as web servers, email gateways, FTP servers, web proxy servers, remote access servers.
3. Medium Trust (Enterprise/Extranet) - The Enterprise zone is where end-user systems reside, including end-user workstations, printers. Endpoint protection is critical to limit the exposure of end-user systems to malware.

12. Functionality at Network Layer

The network layer ensures channel security and has to implement the controls as per the security policy at the network layer.

1. Network Access Control (NAC) – Provide endpoint security technology, the user or system authentication and security policy enforcement.
2. Intrusion detection system (IDS)/Intrusion prevention system (IPS) - IDS monitors a network or systems and identifies malicious activity or policy violations while an IPS watches network traffic as the packets flow through it and identifies suspicious activity, log information, attempts to block the activity, and then finally reports it.
3. Firewall - Prevent unauthorised internet users from accessing private networks connected to the Internet. Basically, they do stateful packet inspections.
4. Content Filtering - Screen and exclude from access or availability, Web pages or e-mail that are deemed objectionable.
5. Message Security - Message security uses the WS-Security specification to secure messages. i.e., ensure confidentiality, integrity, and authentication at the Simple Object Access Protocol/SOAP message level (instead of the transport level).
6. Wireless security – Prevent unauthorised access to the network using wireless networks. Common protocols used are Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA).
7. Remote Access Security – Implement remote network access safely and easily to a wide range of users and devices.
8. Data Loss Prevention (DLP) – DLP makes sure that end-users do not send sensitive or critical information outside the system network. It also describes software/services products that help a network administrator control what data end users can transfer.

13. Application Layer

To ensure the smooth running of the production set-up, maintaining a separate development, testing, and staging environment is recommended.

The technology selection should be done to help to provide better security along with the performance.

Every application should go through vulnerability assessment and penetration testing before making it available in the production setup. VAPT is carried out by external agencies. VAPT should be carried out at a regular interval and whenever any new patch or functionality is added or removed from the service/application.

The comprehensive application is required to be developed in strict accordance with the guidelines laid out in the Guidelines for Indian Government Websites (GIGW) versions 2.0 and 3.0.

14. Functionality at Application Layer

Below functionalities should be provided at the application layer to secure the service/application and its data:

1. Static testing and code review - The purpose of this type of testing is to identify the vulnerabilities without carrying out the actual execution of the code. The development or implementation team does this testing and provides the reports related to the same.
2. Dynamic application testing- The purpose of dynamic application testing is to determine the associated security vulnerabilities in the code by executing it. This helps to identify the security issues related to the complete production set-up including the exact version of the application and application stack.
3. Web application firewall: Firewalls at the application level should be given consideration to prevent the attacks such as SQL injection, Cross-Site Scripting (XSS), cross-site request forgery etc.
4. Vulnerability assessment and penetration testing(VAPT): The objective of carrying out the VAPT is an identification of vulnerabilities and possibilities of their exploitation. A policy should be defined by SI to foresee the possible vulnerabilities and simulation of exploiting those vulnerabilities. The policy should address the guidelines VAPT at regular intervals should be carried out to exploit the vulnerabilities associated with configuration changes at various levels, i.e., network, application server, database servers etc. Vulnerabilities assessment should also be carried out w.r.t possibility of execution of malware, viruses etc. and should be defined in the policy.
5. User Authentication: There should be a proper authentication mechanism being implemented in the applications for providing access to sensitive information to the users.
6. Database monitoring- Monitoring the application, database servers for their uptime, threats, user access management with foot printing & audit trail logs for actions which are being observed.
7. Error Code Index: Error Codes need to be defined & indexed in the system so that the user understands what's the error in the system, and whom to reach out to resolve the error.
8. Role/Rule-based access: A proper authorization policy and rules should be defined to prevent unauthorised access to the various areas of the application.

15. Controls at Application Layer

1. Applications should not be made public unless and until tested for security.
2. A regular audit should be conducted of the application/service.

Avoid unwanted access.

16. User Authentication:

Users should be authenticated with a strong authentication factor based on the sensitivity of the application/service as well as data.

Application Access Control/User Access Management

Objective: To ensure authentic access to the systems and services/applications.		
1.	Registration and Deregistration	Only authorised users should be allowed to access systems and services. In order to identify the authorised users, a facility of registration and de-registration should be provided for every service. This will help enable the appropriate access rights.
2.	Access Provisioning	A formal access provisioning of the users should be implemented. It will assign or revoke the access rights for the users.
3.	Authentication Mechanism	The users will have to pass through an appropriate authentication mechanism such as password, OTP, Digital Certificate, Remembering Browser, etc to access the services. Access can be controlled based upon the data and service sensitivity and in accordance with the security policy.
4.	Secured Log-in process	Every service/application can be accessed only through the secured log-in mechanism based on the chosen authentication mechanism.
5.	Password Management	Password management systems should be interactive and should ensure quality passwords. The password management systems should also be secured and should have a provision such that no password can be leaked.
6.	CAPTCHA Management	CAPTCHA version which shall be used in the project shall not have any user interaction. It shall be just behavioural analysis, so there is a frictionless user experience and enables reCAPTCHA to better detect fraud by comparing all manner of transaction behaviour. The supplied version of reCAPTCHA should allow integration with an API-based service, should have SLA so that it doesn't become a bottleneck while the user is trying to business operation on the platform.
7.	Access control to source code of the program	Access to program source code should be managed in secure environment.

8.	Management of Secret authentication information of the users	Secret authentication information of the users should be managed as per industry standards. The information storage should comply with the acts/laws related to storing the secret information of the user.

Table 8: User authentication controls

i. Authorise:

Though the user is authenticated, she/he may not be authorised to access certain systems, data, information, services. Every information and information providing facility should be accessed only by its authorised users.

The access rights usually are time-bound and should be verified on a timely basis to avoid unauthorised access. The change in the business processes should immediately reflect in the authorization policy and be implemented on priority to avoid unwanted access. For implementing authorization along with multi-factor authentication rules or role-based access should be provided to the users.

17. Logging and Monitoring:

Objective: To record events to create evidence.

1.	Log creation	Events such as user activities, failures, exceptions, information security events, server, firewall, IT equipment transactions etc. should be recorded and maintained in the log format. System administrator, system operator activities also should be logged and protected.
2.	Protecting logged information	These log files are important evidence and should be maintained and also secured from hacking. An encryption mechanism can be used to protect log files from unauthorised access and tampering.
3.	Clock synchronisation	The reference point for all the activities, events, logging is time and hence the clocks of all the relevant systems should be synchronized.

Table 9: Authorization controls

18. API Security

It is possible to attack or leak the data in transit while calling the API and hence the API design is equally crucial when talking about security. Following care must be taken while designing API:

1. Information required for routing or interpreting the contents of the packet should be part of the header and should be appropriately tagged.
2. The body of the packet should be encrypted and should not be easily accessible. The user's information should be part of the body of the packet and not the header.
3. Provide some default value for optional parameters/tags.
4. Only necessary information should be taken from the user and unnecessary information exchange should be avoided.
5. Preferably no personal information should be shared as a part of the response.
6. API should be made available only on the secured channel.
7. Access to API should be provided only to authorised users.
8. Whenever data is exchanged between two servers, it should be done only after proper whitelisting of the IPs; requests should not be accepted from any other IPs.

19. Data Layer

Data is the most crucial aspect of security and should be protected in multiple ways. Classify the data as per its sensitivity level (Highly sensitive, medium sensitivity, not sensitive). Appropriate methods should be chosen while storing the data in the database, files, directories, or any other mechanism. Based on the level of sensitivity the policy should be chosen for storing the data. Various mechanisms can be encryption, hashing, and maintaining in clear text format. The storage location is also dependent on the sensitivity of the data.

Access to any of the data should be provided through APIs or through proper authentication and authorization. The transport of data on various channels also should be ensured for security.

i. Functionality at Data Layer

1. Data needs to be secured when at rest, at motion i.e., in transit or in use – Every piece of data irrespective of its sensitivity needs to be secured against the threats of unauthorised access, data corruption or complete data loss. Depending on the sensitivity and availability needs, methods should be applied to secure the data.
2. Identity and access management for data – The data should be accessible to only authorised persons, at the appropriate time and only for the specified purpose.
3. Access Right Management – Access to data should be restricted by creating and applying a policy for every kind of data set. Data access policy will define the constraint for controlling the data access by its users. It will help in applying appropriate read, write controls over data elements.
4. Data Integrity monitoring – Data Integrity is as important as any other aspect of data security. If the correctness of data cannot be determined, it is almost the same as data loss. In some cases, having data with compromised integrity is more dangerous than having no data. Therefore, a mechanism needs to be applied to monitoring data integrity at various stages to enhance authenticity, reliability, and availability of data.

5. The requirement results in the appropriate access control for data. Regular monitoring, logging, auditing of data is required. A backup plan should be prepared and implementation as per the plan should be ensured as per industry standards.
6. Data should be classified as per its sensitivity and the appropriate rights should be imposed for the modification of the data.

ii. Controls at Data Layer

Controls at every layer of the data should be ensured using proper data governance framework as designed by the SI in consultation with PFRDA.

iii. Backup:

Objective: To protect data against data loss.

1.	Policy Creation	A backup policy should be created and documented to create the backup of the data, information, system, and software.
2.	Information Backup	Regular backup should be scheduled for applications, systems, information, and data as per the backup policy. The backup should be tested regularly to verify its integrity.
3.	Backup protection	Backups should also be maintained in the encrypted format to protect its integrity.

Table 10: Data layer controls

iv. Security Standards

1. ISO/IEC 27001:2013, ISO/IEC 27002 are referred for defining the control objectives and controls. These standards are followed in the organisation for defining, implementing, and monitoring information security at various levels. The standard elaborates on the controls at management, user access control, key management and cryptography, human resource management, system, and application access etc. It is best practice to follow the controls given in these standards to ensure information security in systems, applications and information facilitating assets in the organisation.
2. ISO/IEC 27002 is referred to as a guideline while designing this document. The standard also provides guidelines to design controls for organisation-specific security requirements.
3. NIST SP 800- 30 is referred for defining risk assessment and risk management.
4. Cloud Security Standards by cloud standards customer council is referred for providing suggestions regarding controls for cloud environment.

v. Application layer

The Application layer should comprise of 4 essential sub-components:

Microservices provide a great way to increase cohesion and loose coupling, the client layer is also benefiting from such architecture. There are 2 main components of application layer:

1. Micro Front – end architecture layer: The architecture of the Application Layer will be designed using a micro-apps strategy.
2. Micro apps should be compatible and flexible to be evolved without dependency on other apps simultaneously should maintain the system consistency and user experience.
3. Usage of modern web framework to define client layer adhering to micro frontend architecture and to avoid tight dependency between parent – child component. Popular frameworks which are available in the market - Angular, React, Vue, etc.
4. Data sharing between micro apps should be separated to a shareable data layer through query params, browser storage capability like session-storage, cookies, or indexed DB to store complex data structure.
5. Compatibility to be maintained between various apps, so that micro-apps can be evolved without being dependent on other apps and not break overall system consistency or break user experience.
6. The target architecture should adhere best practice via workspace, projects, and libraries.
7. Design of complex web app to be build using micro frontend by splitting based on feature or domain.
8. Separate codebase for each micro frontend under CI-CD pipeline
9. Micro frontend apps should be bundled and served together with a web app shell.
10. Micro-app layer :App layer should ensure application specific business logic, and data shaping needs are not force-fitted into the micro-services layer.
11. Micro-services layer should remain truly reusable and driven by the domain model/business architecture.
12. All the app specific customization to a domain model property influenced by screen design to be extracted from domain logic to app-specific layer.
13. App specific services layer is expected to provide the necessary decoupling in the architecture.
14. App layer should also provide the customization configuration needed for the presentation layer such as mandatory and optional form validation rules, visibility of fields based on use case or tenant needs.
15. The design should provide flexibility in configuring the application layer look and feel. The configuration would include UI themes, fonts, font-sizes, colours, logos, and the likes.
16. Application layer should be modular enough so that code customizations be feasible by individual components to make UI level changes.
17. Target platform should be built from API first approach ensuring the same set of endpoints exposed by services can be consumed by different channels.

vi. Platform layer

The Platform layer should comprise of 9 essential sub-components:

In case of Multi-tenant, Multi rule:

1. Each tenant may have different rules, and to that extent the platform design will need to provide for tenant specific rules.
2. The rules should be data driven to the extent possible, however, not all requirements for rules customization can be fulfilled via data configuration.
3. The platform design needs to allow for simple code extensions/plugins can be coded if needed.
4. The target architecture should support multi-tenancy using a separate database for each tenant model. The connection parameter for different database instances can be configured in the central tenant registry which stores all the meta info of the tenant.
5. The architecture should ensure connection parameters for different database instances to be configured in the central tenant registry which stores all the meta info of the tenant.

Role based Access control (RBAC) and Attribute Based Access Control (ABAC) features:

1. System should implement role & privilege -based access control.
2. Roles should be externalised from the services - It should be possible to create new roles using data configuration and give relevant rights to the role also using data configuration.
3. System should also implement attribute-based access control.
4. Systemic controls also should not be hard coded in the services but be implemented via interfaces/service extension code.
5. All the endpoints exposed by a micro-service or a consumer listening to an event should be controlled by a defined authority to implement role-based authorization.
6. Roles should be defined based on a set of authorities and should be validated by a policy evaluator mechanism.
7. Authorization system should be robust enough to add/revoke any end-point access without a need of deployment.

OAuth features:

Security being the most crucial part of the system, authorization should be dealt with utmost care.

1. PKCE (Proof Key of Code Exchange), an extension to Authorization code Flow should be used in the OAuth2.0 authorization framework.
2. OAuth should be implemented by a separate authorization server.

3. A well-defined and tested tool for IAM (Identity Access Management) provider should be used.
4. Identity service should have dynamic token-based communication with state information.
5. Service should ideally verify the information in the JWT token verification. Reverse proxy-based token verification would provide external users to have a first pass on the reverse proxies.
6. Identity and access management platforms should in turn provide resource information for each service resource.
7. Implications of zero trust environment should be considered as guidelines for target architecture.

Metrics, KPI and Analytics features:

1. The platform needs to have a solid BI and analytics framework. In order to provide robust way of making data driven business decisions, cross functional workflows and to establish growth metrics across the time frame.
2. Based on the domain model and business architecture, processes and KPIs for the processes need to be identified.
3. Thresholds and targets need to be set for KPIs and metrics.
4. Appropriate data modelling needs to happen to calculate and capture summaries incrementally and provide high performance reports.
5. Analytical reports should not be run off OLTP schemas and hence a separate read only schema should be configured known as OLAP.
6. The data model for OLAP should be a flat schema as far as possible for faster querying without bearing the cost of JOINS (in case of RDBMS).
7. Proper dimensional model design with proper facts, dimension, attributes, fact table, dimension table for BI attributes.

Performance:

1. Effective performance using infrastructure as a code in order to provision new resources in case of high load transactions.
2. Performance engineering should be adopted as a methodology at various steps:
3. Logging of queries to database server, their execution time while development to identify slow traces and poor performing queries.
4. Performance testing using enterprise tools to measure the load threshold of service under fully loaded DB and empty DB.
5. Presence of Infrastructure as Code automation to provision resources automatically when load increases and services require more computational resources.

Base platform:

1. The platform needs to provide a set of base libraries that enforce such cross-cutting concerns on the service/data table in question so that impact of human error in coding is minimised.
2. Definition of audit fields across the entities, common models, endpoints which might be required by all domains should be a part of the platform-base and it should be available to all microservice via a dependency.
3. Definition of data archival design as per the archival policy(hot, warm, and cold storage)
4. The target platform should support multiple service-bases for different domain services requiring different schemes of databases such as RDBMS.

Future Expansion

1. The scope of this e-PLATFORM primarily encompasses a browser neutral & device agnostic web application. However, it is essential to recognize the potential for growth and evolution in the future. To ensure the long-term viability and scalability of the solution, we expect our selected SI to plan for multi-language support and mobile app integration/development, although these aspects are not part of the immediate scope of this project. **Multi-Language Support**: The solution must be designed in a manner that can seamlessly accommodate multi-language support as a futuristic requirement. This includes implementing a content management system or architecture that can handle translations, localization, and cultural adaptations as necessary.
2. **Mobile App Development/Integration:** The solution must be designed in a manner that in future if a mobile application is to complement the solution, SI to ensure that the core components or APIs developed during this project are mobile-ready and can be easily integrated into a mobile app interface.
3. Integrating AI and ML Technologies: The proposed solution must be designed with a flexible and robust integration technologies allowing seamless incorporation of AI and ML tools via the API studio. This design should be inclusive of a wide array of programming languages and coding methodologies ensuring capability regardless of the programming language used in developing the PFRDA e-platform. This feature is crucial for ensuring the solutions, adaptability and scalability in line with future technological advancements.

2. Solution Components and Software Stack

i. Guiding Principles

It is preferable to deploy open-source solutions to build PFRDA new system, which is modular, scalable, and portable across platforms. All the platforms and solutions proposed for PFRDA system should be vendor neutral and PFRDA should be able to replace any platform without any constraint.

We understand that there may be certain components that have significantly stronger commercial/SaaS solutions compared to open source. Examples include API gateways, and certain DevOps components which follow open standards. In such cases, a commercial component may be proposed. Cloud native solutions are not allowed.

ii. Definitions

Technology Type	Definition	Expectation
Open-Source	For any component to be called Open Source, complete source code should be provided to PFRDA under a perpetual, global, irrevocable, royalty-free licence that allows PFRDA to use, modify, exhibit, and redistribute the code.	Open-source components are preferred as part of the Technology Stack. Any updates to an open-source software as a result of the enterprise support of the same will be added back to the community. Enterprise Support for open-source components is required. Bidders may provide Enterprise Support via its inhouse COE. For the avoidance of doubt, Enterprise Support is different from Enterprise Version of open-source components.
Enterprise Edition Open-Source or Enterprise Version Open-Source	Enterprise Version is where a fork has been created by an Enterprise and proprietary enhancement have been made, such that one or more of the below is true: - the source code of those proprietary changes is not available to the general software developer community. - the source code of those proprietary changes is not available to PFRDA. - the proprietary changes are chargeable under a licence fee. - the proprietary changes have resulted in a roadmap deviation from the original open-source product	Enterprise Editions/Versions of open-source software components are not encouraged. However, if there is a strong case for it, bidders may table the same.

Technology Type	Definition	Expectation
Bidder Solution Accelerator	Existing code or products owned by bidder that bidder believes will benefit PFRDA platform and is willing to do IP sharing with PFRDA. Bidder Solution Accelerators can be used wherever Bespoke is allowed, as long as the IP sharing clause is met.	IP Sharing Clause for allowing used of Bidder Solution Accelerator: Such Solution Accelerators owned by bidder may also be used as long as: - they fit the functional needs as expected, including extensibility. - they are technically robust. - a well-defined roadmap exists for product improvement and Bidder can demonstrate that resources have been allocated towards the same independent of PFRDA project
Open Source as Managed Service	This is where CSP provides an Open-Source product as a Managed Service. The value added could include auto-replication, backups, clustering, fault-tolerance, managing uptime, etc.	These are allowed where explicitly mentioned in the table below. For each of the "Open Source as Managed Service" components, Bidder is expected to list out the specific Open-Source Community Edition software used as part of their RFP response. Any Cloud Native functionalities that are not as per the value-added services listed earlier will not be used in building the solution. For example, in case of RDBMS - Bidder may use the backup, replication, clustering like facilities but if there is a Cloud Native specific query language to query the Managed Service RDBMS in question, that may not be used.
COTS or Proprietary	This includes 3rd Party commercial software, PaaS, and Cloud Native components	These are allowed where explicitly mentioned in the table below.
Bespoke	Bidder will write custom code to build the Platform	
Cloud Infrastructure	Govt. Approved Infra only	MeitY Empanelled CSPs with GCC & VPC will be allowed.

iii. Preferable Technology Types

An indicative list of solution components has been provided below. The Solution Components in the list have been identified as Core and Non-Core. For each solution component, the requirement in terms of Open Source/Bespoke/Proprietary is also given in the table below. Enterprise support, from respective OEMs, is required in India for all the solution components mentioned in below table, as applicable.

S.N.	Solution Component	Type
1	Help Desk and Incident Management	Functional

S.N.	Solution Component	Type
2	Digital Compliance, Regulatory Business Process, RegTech Access for all Intermediaries, Supervisory Business Process, Compliance	Functional
3	API Gateway	Technology
4	Application Server	Technology
5	Build Management	Technology
6	Content Delivery Network/CDN	Technology
7	Containerized infra	Technology
8	Database (RDBMS/non-RDBMS)	Technology
9	DevOps tools	Technology
10	Event Stream Engine	Technology
11	In Memory-Caching	Technology
12	Logging	Technology
13	Notifications (including Push, SMS)	Technology
14	Operating System	Technology
15	Queue-based Messaging	Technology
16	Rules Engine	Technology
17	Search	Technology
18	Source Control	Technology
19	Web Server	Technology
20	Workflow Engine (BPMN Compliant)	Technology
21	ETL	Technology
22	Load Balancer	Technology
23	Monitoring Services	Technology
24	NAT Gateway	Technology
25	Patch Management	Technology
26	Security Software, including Firewall	Technology
27	VPN	Technology
28	Master data management (MDM)	Techno-functional

S.N.	Solution Component	Type
29	MIS Reporting	Techno-functional
31	Analytics Tool	Techno-functional
32	BI Tool	Techno-functional

Solution Components

It is understood that there may be other components that may be needed to build the overall system. In such a case, bidder may propose Open Source or Proprietary, however the preference remains for open-source components.

Furthermore, bidder should ensure that none of the open-source components/products or any other IP used by bidder to build PFRDA platform shall have any restrictions that prevent commercial usage of PFRDA platform, and the said components/products shall not impose any limitation to use by PFRDA.

3. Non-Functional Requirements - Parameters for Performance and Scalability Testing

SI shall use the below parameters to conduct performance testing of the system as part of QA testing. Test Data setup will be done accordingly so that the Test DB reflects real life data volume as well as real life system load. Mock transactions may be made where relevant to set up such a Test DB.

i. Setup Parameters for setting up Performance Testing DB

Setup Parameters	Value
Number of External Users	5,000
Number of Internal Users	1,500
Number of BI Users	1,000
Number of Records	100 Million
Volume of Data in Reporting Subsystem	100 -150 GB

Table 11: XXX

ii. System Load Parameters that define what load to exert on the system during performance test.

System Load Parameters	Value	Remarks
Concurrent Users for PFRDA e-PLATFORM	1000	"Concurrent Users" refers to the total number of users simultaneously accessing a PFRDA resource such as an API endpoint.
Concurrent Users for BI	50	
Concurrent Users for Canned Reports	100	
API hits per second	1000	
Number of Hours in a Day	8	
Peak Load Hours/Day	2	
Peak Load to Average Load Ratio	2	
Network latency	100 milliseconds	

Table 12: XXX

iii. Performance Targets

Parameters	Value	Remarks
Page Rendering on App	2 seconds	Cumulative of API response time, data transfer on the network, and rendering the page on the App
API response time (95 percentile)	1 second	
Reports Load Time – Simple Report	2 seconds	
Reports Load Time – Medium Complexity Report	4 seconds	
Reports Load Time – Complex Report/Dashboard	8 seconds	
Uptime	99.5%	

Table 13: XXX

4. Software Build, Integration and Testing

#	Key Responsibilities	SI	PFRDA
1	Execute automated static code analysis and verify no blocking or major issues are detected	X	
2	Manual code review, to verify the code quality and to verify if code is compliant with agreed conventions, standards, and best practices	X	
3	Possibility to participate in the code review		X
4	Develop an overall test plan that documents the test strategy, test coverage, test scenarios, test bed, test data, test methods, test schedule and responsibilities to accomplish quality assurance of the affected system	X	
5	Provide and manage a test environment with either scrambled real-time production data or relevant generated test data. This test environment should allow the execution of all test categories defined in this section.	X	
6	Mask the test data for sensitive information	X	
7	Create test cases and suitably use the existing data as well as analyse the new use cases to generate new test data to perform all appropriate testing, including Functional Testing (including positive, negative, and boundary value based testing), Assembly/Integration Testing, End-to-end Testing, Performance Testing, Scalability Testing, Failover Testing, Reliability and Soak Testing, Stress Testing, Regression Testing, Cross-browser/platform testing, Security Testing, including Vulnerability Assessment and Penetration Testing (including OWASP Top 20). Note: Collectively these various testing types will be referred to as “System Testing”	X	
8	Conduct technical smoke tests	X	
9	Conduct functional smoke tests, e.g., story testing	X	
10	Support functional smoke tests & User Acceptance Testing		X
11	Conduct Regression Testing per test plan requirements	X	
12	Conduct System Testing per test plan requirements. For scope of System Testing, see point #7 in this table	X	
13	Conduct cross-browser/cross-platform testing if appropriate	X	

#	Key Responsibilities	SI	PFRDA
14	Automate test scenarios as much as possible, to a certain extent. Achieve minimum 80% code coverage via test automation	X	
15	Provide shared access to the mutually agreed defect tracking system for purposes of allowing PFRDA to initiate, track, and the report found defects (e.g., user acceptance testing)	X	
16	Correct defects found as a result of testing efforts	X	
17	Develop, document, and maintain in the Policies and Procedures Manual integration and testing procedures that meet PFRDA requirements and adhere to policies defined by PFRDA	X	
18	Maintain software release metrics across development, quality assurance, and production environments and networks	X	
19	Provide and support in-scope application associated middleware required to integrate software and services	X	
20	Perform configuration management and Change management activities related to integration and testing	X	
21	Continuously improve the testing services, for example by introducing new automated test approaches or any other improvements	X	
22	Maintain document repository with all relevant documents stored in a structured manner with proper version control	X	
23	Establish automated code quality measurement via static code analysis using standards agreed with PFRDA during Baselining Phase	X	
24	Work with PFRDA to obtain and deploy the appropriate infrastructure required to set up new domains or subdomains to host new systems, including procuring and setting up the SSL as per government approved guidelines.	X	
25	Ensure the system is accessible via PFRDA Website, via a subdomain or other standard industry practices.	X	

5. Software Change and Version Control

1. All configuration changes or customizations or bug fixes or enhancements in the functional scope mentioned in this RFP for the proposed application, which do not involve the creation of any new application process, are to be carried out by the System integrator at no extra cost.

2. Changes in the application software which are mandatorily required for complying to any of the predefined SLA requirements, FRS or To-be Functional solution cannot be treated as a separate Change Request, and hence are to be completed by the System integrator at no extra cost.
3. All changes during the warranty phase shall be subjected to comprehensive and integrated testing by the System integrator to ensure that changes, implemented in the system, meet the desired and specified requirements of PFRDA and don't impact any other function of the system.
4. The System integrator shall submit a Quarterly Report on the changes performed on the application and resolution of malfunctions carried out by the System integrator. Application documentation is updated to reflect on-going maintenance and enhancement including Software Design Documents and SRS, in accordance with the defined standards.
5. All the scope & objective should be documented, approved by PFRDA in conception & implementation during the entire project & be available to be produced during the entire project duration.
6. Details the functionalities and features expected from the software change and version control system. This could include aspects like (indicatively):
7. Support for version tracking, branching, and merging.
8. User access controls and permissions.
9. Integration with development tools and IDEs.
10. Notification and alerts for changes and updates.
11. Audit trail and logging of changes.
12. Any technical specifications the software change and version control system should adhere to, such as compatibility with specific operating systems, programming languages, and databases.
13. Change management workflow and processes should be followed properly. This could include:
14. Submission and approval of change requests.
15. Testing and quality assurance procedures.
16. Deployment and release processes.
17. Handling of rollbacks and emergencies.
18. If the software change and version control system need to integrate with other tools or systems (e.g., continuous integration tools), outline the integration requirements and any relevant APIs.
19. Proposed solution & approval from PFRDA needs to be taken every time to state security expectations, including encryption, data protection, and user authentication mechanisms. PFRDA should approve on how user access will be controlled and managed.
20. Any change in the reporting and analytics features, or the types of reports that PFRDA expects should go through a software change and version control system to generate.

21. The ITIL (version 4) process should be followed by SI to outline how maintenance, upgrades, and bug fixes will be handled by the vendor, including the frequency of updates.
22. SI should clarify & get approval on the ownership of the software change and version control system, and specify the licensing terms, whether it's a perpetual licence, subscription-based, or open-source solution, IaaS, PaaS, SaaS, etc - for each and every component used in the entire solution architecture.

End of document